An Archeology of Cryptography: Rewriting Plaintext, Encryption, and Ciphertext

By

Isaac Quinn DuPont

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy
Faculty of Information
University of Toronto

An Archeology of Cryptography: Rewriting Plaintext, Encryption, and Ciphertext

Isaac Quinn DuPont
Doctor of Philosophy
Faculty of Information
University of Toronto

2017

Abstract

This dissertation is an archeological study of cryptography. It questions the validity of thinking about cryptography in familiar, instrumentalist terms, and instead reveals the ways that cryptography can been understood as writing, media, and computation.

In this dissertation, I offer a critique of the prevailing views of cryptography by tracing a number of long overlooked themes in its history, including the development of artificial languages, machine translation, media, code, notation, silence, and order. Using an archeological method, I detail historical conditions of possibility and the technical a priori of cryptography. The conditions of possibility are explored in three parts, where I rhetorically rewrite the conventional terms of art, namely, plaintext, encryption, and ciphertext. I argue that plaintext has historically been understood as kind of inscription or form of writing, and has been associated with the development of artificial languages, and used to analyze and investigate the natural world. I argue that the technical a priori of plaintext, encryption, and ciphertext is constitutive of the syntactic

and semantic properties detailed in Nelson Goodman's theory of notation, as described in his *Languages of Art*. I argue that encryption (and its reverse, decryption) are deterministic modes of transcription, which have historically been thought of as the medium between plaintext and ciphertext. By developing a new understanding of encryption as standing *between* two agents, I characterize the process in terms of media. As media, encryption technologies participate in historical desires for commodious and even "angelic" transmission, popular until the twentieth century. I identify how cryptanalysis, or "code-breaking," is distinct from cryptography, and instead relates to language, being associated with the history of machine translation. Finally, I argue that ciphertext is the perspectival, ordered result of encryption—similar to computation—and resists attempts to be spoken. Since ciphertext resists being spoken, its application problematizes the category of language, and has, at least once in antiquity, been considered a means of creating silence.

This dissertation is the first of its kind to offer a historically-rich, ontological analysis of cryptography, which therefore opens the topic to new fields of scholarship and humanistic forms of inquiry.

Acknowledgement

Many colleagues and friends have given me invaluable assistance and support over the years I worked on this dissertation. My committee, Brian Cantwell Smith, Patrick Keilty, Yuri Takhteyev, and Brett Caraway, has for many years challenged me, supported my work, and provided a haven for intellectual curiosity. I would also like to thank my defence examiners, Anthony Enns and Costis Dallas, who provided exemplary critique and feedback.

This dissertation is not only the product of my time at the University of Toronto. Without my friends and colleagues at the University of Victoria and Western University I would not have been prepared to undertake this work. Through these formative years many people have offered me encouragement and support, especially my undergraduate colleagues in philosophy, and my graduate colleagues in library and information science. I am also thankful to have learned a great deal from my many academic mentors over the years, especially Bill Maurer and Taneli Kukkonen.

I am fortunate to have received funding from a SSHRC Doctoral Fellowship, two Ontario Graduate Scholarships, an Enhanced MITACS Accelerate Fellowship, and a Litwin Books Award for Ongoing Doctoral Dissertation Research in the Philosophy of Information.

My many friends through the years have been unwavering in their friendship and support, especially Bradley Fidler, Robyn Lee, Clayton Lewis, Sean Rupka, Ashley Scarlett, Hannah Turner, and of course, Rory. My family has always encouraged my intellectual goals, but none more than my sister, Michelle Vingo. I owe my greatest debt of gratitude to Alana Cattapan, to whom this dissertation is dedicated.

Table of Contents

Part One: Plaintext

Part Two: Encryption

Part Three: Ciphertext

List of Figures

List of Appendices

1
Towards ubiquitous cryptography

> *Under the conditions of high technology, literature has nothing more to say. It ends in cryptograms that defy interpretation and only permit interception.*[1]

Two events separated by twenty years punctuate the public's recent interest in cryptography: the 1993 announcement of the Clipper Chip and the 2013 global surveillance disclosures by Edward Snowden.

The early 1990s were a time of significant interest in cryptography. Global telecommunications networks were well established and increasingly vital to daily activities in the developed West. Broadcast signals, such as radio and television, were ubiquitous and reached virtual saturation. Point-to-point networks, such as telephone and Internet networks, had also become critical to business and personal life. For example, by the early 1990s, automated teller machines shuffled a considerable portion of personal and consumer money across private or public telephone lines, and bank-to-bank or business-to-business financial transactions were globally networked and pervasive.

Or consider the birth of the Internet. From the early 1970s, the Arpanet was designed in concert with early networked encryption technologies, in which cryptography technologies were built into the online "hosts" sitting at the edges of the network architecture.[2] Because of these early decisions about the placement of security features in the architecture, once the Arpanet transitioned from its military-funded university roots to the global Internet, it lost its existing encryption technologies and would have become necessarily open and susceptible to eavesdropping. But, on the Internet, with burgeoning personal and commercial uses very much in want of strong cryptography, the Data Encryption Standard (DES) and commercial forms of public key cryptography were developed to fill the vacuum left when military encryption was no longer a possibility.

In the same era, telephones shifted to a digital, publicly-switched telephone network, first with the introduction of digital system switches and core services, and eventually, digital terminals. In the early 1990s, the US government promoted the development of secure digital telephony for state and corporate

[1] Kittler, *Gramophone, Film, Typewriter*, 263.
[2] DuPont and Fidler, "Edge Cryptography and the Co-Development of Computer Networks and Cybersecurity."

applications. In 1992, AT&T produced a telephone encryptor (TSD–3600-D), a device positioned between the telephone terminal and the open telephone network, utilizing a 56-bit DES encryption algorithm. Since the Internet was already rapidly deploying cryptography at this time, the US government was looking to head off a world in which strong cryptography would prevent state surveillance. The US government announced the "Clipper Chip,"[3] a security module to be used in a new model (TSD–3600-E) of AT&T's telephone encryptor product line. The Clipper Chip version of the telephone encryptor enabled state and law enforcement agencies the ability to tap a phone and circumvent the cryptographic protections, which otherwise kept conversations private between the communicating parties. The plan was that once the chip was produced, the US government would generate the necessary cryptographic keys and hold them in escrow until lawfully requested, at which point the keys could be used to decrypt the transmitted data from the selected device.

Prior to the release of the Clipper Chip, few people understood cryptography, seeing little need or having little desire for what was thought to be a spy and war technology. Around the same time the Clipper Chip was launched, Phil Zimmerman created a system for encrypted email, called Pretty Good Privacy (PGP), thereby defying the US government's decision to label cryptographic materials a munition, and providing security and privacy for digital communications. Zimmerman understood that email was rapidly replacing the postal system (already a foregone conclusion by the late 1990s) and that interception on open networks was trivial—as easy as it was to intercept radio signals in World War II.[4] To shift privacy back into the hands of the sender, Zimmerman's PGP ensured that no government could cryptanalyse (or "crack") encrypted email messages. Zimmerman made his program freely—and importantly—*globally* available, in defiance of export controls on strong cryptography. Between PGP, the birth of the Internet, and the Clipper Chip, the political fight that ensued came to be known as "the crypto wars."

The Clipper Chip was a move by the US government to sate the public's desire for Privacy Enhancing Technologies (PETs), while ensuring police and intelligence agencies would not be shut out from surveillance on the emerging networks. The hope was that Clipper Chip technologies would proliferate and ensure privacy among businesses and individuals, but when lawfully required still permit surveillance. The public saw it differently. In June, 1994 the interest

[3] The chip was designed by Mykotronx and manufactured by VLSI Technology, formally known as the MYK–78.
[4] Zimmerman, "Why I Wrote PGP."

in emerging cryptography was so great that it became a matter of genuine public interest; Steven Levy wrote a popular article on the topic for the New York Times. His article, "Battle of the Clipper Chip," described the emergence of "high-tech Paul Reveres" who go by the name "Cypherpunks." Levy wrote about Tim May, honorary leader of the political movement, and co-founder of the mailing list Cypherpunks, who remarked, "the war is upon us," and then made obligatory reference to George Orwell's *Nineteen Eighty-Four*. The outlandish cypherpunk arguments of that day are now, today, strikingly familiar, even quotidian: the government should not surveil the innocent; the government has no business in personal affairs; and, (reflecting then-emerging cyber-libertarian views) the government has no right treading on the wisdom of capitalism through its heavy-handed control of technology. To make matters worse for the government, it was quickly discovered that the Clipper chip's cryptographic "hash" (a kind of "digital signature" used to authenticate the Law Enforcement Access Field), the key feature enabling lawful decryption, was too short to provide strong security.[5] Basically, the public didn't want cryptography with a government backdoor that didn't work in the first place. By 1996, the project was abandoned; the cypherpunks had won the battle.[6]

Over the next twenty years, cryptography blossomed into a massive industry. The US government removed cryptography from the munitions list and gave control to the US Department of Commerce. Cryptography was therefore no longer a military technology; late-capitalist industry was free to deploy cryptography for increasingly diverse applications. The technology also matured—becoming computationally cheap, reliable, and ostensibly secure. Public-key cryptography, first invented in the 1970s (in secret by Ellis, Cocks, and Williamson at GCHQ, and then publicly by Diffie and Hellman),[7] was essential to these transformations, as it permitted secure communications without prior arrangement of secret keys. Public-key cryptography was also increasingly used for broader applications, notably, for authentication and data integrity.

Cryptography had finally become banal, common, and workaday, as standards and best practices developed through collaboration between the government, private industry, and academia.[8] Yet, as cryptography became increasingly common, all was not well. Those "in the know" had long been suspicious about

[5] Blaze, "Protocol Failure in the Escrowed Encryption Standard."
[6] Diffie and Landau, *Privacy on the Line*.
[7] Ellis, "The History of Non-Secret Encryption"; Diffie and Hellman, "New Directions in Cryptography."
[8] Slayton, "Measuring Risk."

government involvement and its extensive surveillance capabilities. No one, however, predicted the scope and success of the renewed government cryptanalysis and surveillance efforts, following the crypto wars, which would later be revealed in a series of classified information leaks by Edward Snowden.

Beginning in June, 2013, Edward Snowden, working as a defence and intelligence contractor, released a large cache of classified documents to several news agencies. The Snowden leaks revealed a hubristic US National Security Agency (NSA) in collaboration with global intelligence allies (the so-called "five eyes"),[9] capable of infiltrating and cryptanalysing government, business, and personal data that was previously thought secure. The public was instantly enraged—a rage further fueled by a growing alliance between anti-government, libertarian values and modern technophilia.[10] Moreover, the public was shocked because its heretofore unwavering faith and trust in cryptographic technology was revealed to be misguided, perhaps even rotten to its core.

Despite the popular and political backlash, the software developer community realized that cryptography was not fundamentally broken (or had good reason to believe it not to be). What was also revealed by the Snowden leaks was that some forms of cryptography and some practices were impervious to government attack. Faith in cryptography, at least in some sectors, was actually renewed. Snowden himself said as much: "Encryption does work. It's the defense against the dark arts in the digital realm."[11] Collaborator and fellow leaker Julian Assange agreed, taking on an almost religious tone: "the universe believes in cryptography."[12]

Since the surveillance disclosures in 2013, the software development community has deployed cryptography widely. Prior to the Snowden leaks, however, many software developers were already using cryptography, and there is ample evidence suggesting that if the leaks had not occurred, broader deployment of cryptography would have continued nonetheless, albeit at a less accelerated rate. But the Snowden leaks awoke public interest and provided a catalyst for companies that had been dragging their feet to now broadly and rapidly deploy cryptography, many of which now offer cryptography by default.

---

[9] The signals intelligence portion of the "five eyes" alliance includes US's National Security Agency, UK's Government Communications Headquarters, Canada's Communications Security Establishment, New Zealand's Government Communications Security Bureau, and Australia's Australian Signals Directorate.

[10] Golumbia, *The Cultural Logic of Computation*; DuPont, "Opinion: It's Time to Rethink Polarizing Encryption Debate."

[11] Robertson, "Edward Snowden."

[12] Assange et al., *Cypherpunks*.

Indeed, cryptography had long been used for services that obviously required strong security—bank websites, corporate data protections, and so on—but after the Snowden leaks, companies deployed cryptography for trivial and run-of-the-mill applications. Almost overnight, many online chat, photo sharing, and social networking sites were accessible only through virtually uncrackable secure connections.

For the two years following the Snowden revelations, cryptography was deployed on the Internet at an increased rate. One of the principal technologies for Internet cryptography is the Secure Socket Layer (SSL) protocol, which is typically used whenever a remote computer connects securely to a server (as when a user logs on to her bank's website). While there is no one measure or method for tracking the increasing deployment or use of cryptography on the Internet, a fairly reliable account puts the figure of SSL connections at about 25% before Snowden (June, 2013), to 44% a little over a year later (September, 2014), a 19% gain, year-over-year, in the number of secure connections.[13] The Electronic Frontier Foundation (EFF) also began a campaign of publicly monitoring the deployment efforts of popular websites. Similarly, websites like HTTPSWatch began to programmatically track websites using cybersecurity best practices. Within two years of the Snowden revelations, the EFF also initiated a collaborative project to create a server-side turn-key solution for deploying strong cryptography with minimal knowledge or effort.[14] Around the same time, one of the largest virtual private server providers, Cloudflare, began offering "Universal SSL" for its 2 million customers, free of charge. Wired magazine opined that "it's time to encrypt the entire Internet."[15] And on and on. Hacker and programmer communities now regularly demand that they "encrypt everything!"—including local and ephemeral data, not just data that is transmitted across the open Internet.

One consequence of these changes is that perceptions of privacy changed. Although rarely appreciated by privacy advocates (who typically imagine an early Internet with complete privacy), the idea of privacy is in fact remarkably

[13] See Naylor et al., "The Cost of the 'S' in HTTPS." This report also indicates a doubling of encrypted *upload* traffic over the same period, from 46% to 80%, and a more remarkable increase in encrypted bulk data (rather than individual privacy-sensitive connections for things such as passwords), from about 15% to almost 40%. More recently, data finds that in the year from 2015 to 2016, HTTPS connections *doubled* (Podjarny, "HTTPS Adoption *doubled* This Year."). It should be noted, however, that the greatest single increase in the number of online encrypted transactions was due to Facebook making encryption mandatory, which occurred *prior* to Snowden's revelations.

[14] Electronic Frontier Foundation, "Let's Encrypt."

[15] Finley, "It's Time to Encrypt the Entire Internet."

fungible and historically contingent. Snowden has claimed that he "remember[s] what the internet was like before it was being watched," but this was never true.[16] The Internet started life as the Arpanet, which was a military research tool that included surveillance capacities as a central feature of its architecture (the central switches of many of the inter-networks were run by the US National Security Agency, Central Intelligence Agency, and the Defense Intelligence Agency). As Fidler and I have detailed elsewhere, the Arpanet co-developed with cryptography, forming an architecture and infrastructure we call "edge cryptography."[17] These essential changes deeply influenced the resulting fabric of online technologies. When the Arpanet transformed into the Internet in the early 1990s, it was nominally commercialized, but no less surveilled.[18]

The idea of demarcating private and public spaces first materialized, perhaps, in the Renaissance, by one of the principle architects of cryptography, Leon Battista Alberti (although his thoughts on "privacy" had nothing to do with his work on cryptography). Due to the administration of class-specific home accounting ("*oeconomy*") that emerged in the transition to wealthy Italian city states during the Renaissance, it became important for a (male) family head to control access to knowledge about a family's resources. The principle measure to control this knowledge was to physically secure accounting books; held at first in locked closets, and then on Alberti's recommendation, the books were to be separated by a wall between the husband's and wife's beds, so that the private accounting information could be conceptually and architecturally separated. The locked closet eventually became a separate study ("*studio*") that formed the "true center of the house."[19] In fact, Alberti's architectural invention created a uniquely male kind of privacy, a space for arranging the private affairs of the house that only trusted (male) associates were granted access to. There is even some suggestion that the phrase "coming out of the closet" arises from the context of a private study, forming an intellectual space "beyond that of [hetero-] sexuality."[20] As I discuss in chapter three, Alberti's other famous invention—polyalphabetic encryption—would also be (independently) important for reconfiguring notations of privacy. Originally a product of Alberti's reconfiguration of the *studio*, and then his invention of polyalphabetic

[16] Reitman, "Snowden's Motivation."
[17] DuPont and Fidler, "Edge Cryptography and the Co-Development of Computer Networks and Cybersecurity."
[18] DeNardis, "The Internet Design Tension between Surveillance and Security"; Yost, "The Origin and Early History of the Computer Security Software Products Industry."
[19] Poovey, *A History of the Modern Fact*, 34.
[20] Ibid.

encryption, today, online privacy is demanded and expected, and the relationships between individuals have become necessarily mediated by digital technologies—simultaneously more direct and intimate (private, after all), and yet (perhaps) alienated by cryptographic interventions.

What, then, happens when the accelerated rate of deployment for cryptography and its increasingly diverse use reaches a state of ubiquity? In the future will cryptography cease to function as a security measure, and instead become a common carrier, or even, a medium (as was proposed with the failed effort to make the HTTP2 Internet protocol encrypted by default, thereby collapsing any meaningful distinction between the infrastructure of online communication and online security)? Most software developers feel positively about such a world. Cryptography, they argue, adjusts a skewed imbalance of privacy. A world of ubiquitous cryptography is, according to the prevailing logic: safe, secure, and above all, private. But is this the only outcome?

In this chapter I introduce the subject of cryptography by complicating the straightforward picture we have inherited. I argue that "cryptography" has a long and complicated history that belies any attempts at a singular definition. In fact, throughout this dissertation, I will use the term "cryptography" to metonymically refer to the entire range of complicated associations. Where distinctions can be made without forcing artificial clarity on an otherwise complicated narrative, I will specify "cryptographic technology" or the "field" or "subject" of cryptography, or, I will specify cryptographic processes, such as encryption, decryption, and cryptanalysis. I believe it is important to retain such complexity because my goal in this dissertation is to show how the inherited understandings of cryptography are the result of instrumental rationality that has developed over the last long century. I also introduce my "archeological" method, covered in detail in the next chapter, which specifies the technical conditions necessary for cryptography to emerge in a given historical context.

1.1 Definitions and terminological complexity

As a keyword of my study, "cryptography" is actually a complex of terms, all historically contingent and unstable over time. In the first English usages from the mid–seventeenth century, "cryptography," "cryptology," and "steganography" were interrelated and sometimes interchangeable terms. The terms related to "cryptography" are difficult to pin down because they attach to conceptual categories that are specific to particular epochs, and bring shades of meaning unfamiliar to modern ears and eyes. Moreover, the notion of cryptography spans across and within traditional conceptual categories; for

instance, within the Aristotelian categories of techné, praxis, and epistemé, cryptography seems to blur across all three: functioning sometimes as a practical craft, a know-how, an initiation, and a science. Rarely do we think of these associations when we use the terms of art today.

The word "cryptography" is comprised of two Greek roots: *crypt-* from Greek κρυπτός, meaning hidden or concealed; and *-graphy* from Greek -γραφία, referring to various styles of writing, drawing, or graphic representation. In John Wilkins' *Mercury* (the earliest English-language cryptography manual), cryptography is described as a form of writing in code by way of cipher or written "character," and similarly, Francis Bacon's "biliteral" cipher was a means of "representing anything by anything" through binary writing. Because of these historical uses, its etymology, and (as will become clear in chapter three) its co-development alongside writing technologies, "cryptography," with its focus on writing, is my preferred term for the subject, rather than the more modern "cryptology," which has gained prominence alongside efforts to legitimize its scientific study.

As a place to start the investigation, a rather utilitarian definition of cryptography might be something like the following: cryptography is the deterministic substitution and transposition of discrete symbols. One of the useful features of this definition is that it accurately implies that cryptography cannot use probabilistic or random methods for transformations, qua random, unless such transformations are recorded in some fashion (perhaps in the "key"). Indeed, while forms of entropy are vitally important for the (pseudo-) random number generators used in modern encryption algorithms, it is a common misconception to imagine that this randomness is "transferred" into the ciphertext. A simple thought experiment makes this fact clear: if ciphertext was truly random, how could it be reversed (decrypted)? Only an omniscient god, living in a grindingly deterministic world, could actually decrypt a truly random message (which, of course, would no longer be random!).

Perhaps a slightly better definition of this process of substitution and transposition would invoke combination and permutation. Claude Shannon, for example, defines cryptography as the "set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms)."[21] The "space" of these mathematical sets is produced by their finite discrete structures (studied by the field of combinatorics). Another key feature of Shannon's definition is the *transformation* between mathematical sets, which focuses on the process of encryption. Since the forms of transformation

[21] Shannon, "A Mathematical Theory of Cryptography."

are unique, these kinds of transformations can be used to distinguish between instances or kinds of cryptography.

Encryption is the primary and active mechanism of cryptography—the process of turning plaintext into ciphertext. It has been tradition to demarcate types of cryptography by their encryption mechanisms, but in recent years this focused attention on encryption has increased, as encryption algorithms have become essential and general components, in the sense of being reusable. In order to make the encryption algorithm reusable, it was necessary to develop the idea of a "key." Until the development of an "auto-key,"[22] however, few cryptographers made any distinction between the encrypting algorithm and the key, or, as I describe later, the "index" setting.

Decryption is related to encryption, as its opposite. Whereas encryption turns plaintext into ciphertext, decryption reverses the process, turning ciphertext back into plaintext. In this way, decryption is only as complex as encryption. However, as I describe below, and detail in chapter nine, decryption is quite different from cryptanalysis (or "code breaking"), even if the end result is the same.

What, then, does encryption do, and by extension, what does cryptography do? This seemingly simple question is in reality full of bedeviling complexity, and merely understanding the question is diagnostic of the widespread use of cryptography seen today. Espousing the commonplace view, Shannon believed that encryption created and maintained "secrecy" between communicating parties, and was the sole purpose of cryptography. But in fact, there are many other uses of cryptography, and moreover, there is good reason to think the meaning and articulation of "secrecy" is problematic. Like "privacy," the category of "secret" is complex and fungible. Sometimes "secrecy" attaches to the semantic category of "intentional concealment," but variously, secrecy also includes categories and shades of meaning for privacy, "setting apart," or in the sense of "secrets of nature." The ancient Greek word for secrecy was *arretos,* which first meant unspoken, and thus secret.[23] This word later came to mean prohibited and unspeakable, which added a strong normative sense to the meaning of secrecy, as is sometimes reflected in modern usage. On the other hand, in scientific and artistic domains (distinguished from diplomatic or military uses), cryptographers focused on the power of cryptography to form the basis of a system of "significance" and meaning, while downplaying its use for

[22] Buonafalce, "Bellaso's Reciprocal Ciphers"; Strasser, "The Rise of Cryptology in the European Renaissance."
[23] Long, *Openness, Secrecy, Authorship*, 7.

intentional secrecy.[24] Historically, the connections to secrecy were often backgrounded, and certainly the sense of secrecy associated with premodern uses of cryptography does not mean what it does today.[25]

If we were to assume secrecy is necessarily part of cryptography, how would we make sense of the many strange alliances between cryptography and its historical and contemporary cognates? For example, what would we make of the alliance between cryptography in early modernity and the development of perfect and universal artificial languages and their taxonomic impulses? Or the many other alliances, discussed in the following pages of this dissertation? I argue, against the view that secrecy is necessarily part of cryptography, that cryptography enabled a host of functionalities separate from the idea of secrecy, often related to existing features of language, computation, and communication—including remediation, transmission, temporal linearization, recombination and analysis, and order. Of course, secrecy is not entirely absent here, but its role is downplayed. For instance, for some authors in some epochs, language and/or nature was understood to be veiled, mysterious, and secret. I conclude, at the close of this dissertation, that secrecy plays *an* important role in the functioning of cryptography, but it is actually only one of the many functions of cryptography, erupting when the historical conditions of possibility permit such a configuration, need, and desire.

Whereas the word "cryptography" takes only a noun form, the related term "cipher" is both a noun and verb. Today, the term "cipher" is often used to describe specific encryption algorithms, in the sense of "AES cipher" or "RSA cipher." The word is an adaptation of Arabic "çifr," originally used by Arabic mathematicians to mean zero or nought, or in substantive use, meaning empty or void. As such, its etymology is evocative of the more recent mathematical turn in the study of cryptography.

The old term "character" was once used to refer to cryptographic issues, but no longer retains this meaning. "Character" originally comes from the French "*caractere*," which was used in the context of cryptography to refer to signs, often "natural" or conventional in form. Natural signs made it possible to decipher God's Word and world, whereas conventional or "constructed" signs

[24] Ibid., 110.

[25] Analytically, secrecy is a strange form of communication that requires a considerable balancing of social relationships. In fact, very strong notions of secrecy are self-defeating. As my grandfather once said, "it is only a secret if you don't tell anyone," but of course, this defeats the point of having a secret in the first place.

made it possible to interrogate the human-created world.[26] In this regard, Francis Bacon developed "characters" for his "new philosophy," which required the "ordeal" of experiment to interrogate (even "torture") the natural world. Bacon saw these "characters" as a kind of labyrinth that could be deciphered,[27] but not necessarily interpreted.[28] In fact, cryptography had long been an interest of Bacon's—the "biliteral" cipher that Bacon invented in his youth later provided a functional model for understanding the human role in interpretation of nature. However, as I explore later, Bacon complicated the nature/convention bifurcation. Bacon's deciphering of *nature* was a "mechanical art" that relied on *conventional*, yet "real" (not nominal) symbols.[29]

Throughout most of its history, steganography and cryptography were understood as cognate techniques. Steganography is hidden writing, in the literal sense that steganographic writing has been made hidden or invisible in some sense. Although we now understand cryptography and steganography to be sharply delineated techniques, modern authors writing about the subject would sometimes lump steganography and cryptography together. For example, Edgar Allan Poe explored the literary functions of cryptography through his use of steganography. In *The Gold Bug*, Poe describes "invisible" (or "secret") writing—when a sheet of paper was subsequently and accidently heated near a fireplace it was transformed to reveal its secret contents. Similar kinds of steganography have been common throughout the history of cryptography, with authors concocting special inks created from onion juice, or tattooing images on shaved messengers' scalps, who—once the hair grew back—were then able to deliver messages without detection.[30] In his work on Poe's "cryptographic imagination," Rosenheim offers a modern version of Poe's heat sensitive paper: a JPEG-encoded computer image that is manipulated in a very particular way to hide a secret message within the image's code.[31] Due to redundancy in the JPEG encoding scheme, the image can still be rendered and appears to be nothing unusual, functionally like Poe's paper, but to those who know how and where to look within the image's code, a secret message can be extracted.

---

[26] See Vickers, *Occult and Scientific Mentalities in the Renaissance*, but note that Markley, *Fallen Languages* complicates the natural/conventional bifurcation; see also Bono, *The Word of God and the Languages of Man*.
[27] Pesic, "Wrestling with Proteus: Francis Bacon and the 'Torture' of Nature"; Pesic, *Labyrinth*.
[28] Bono, *The Word of God and the Languages of Man*.
[29] Pesic, *Labyrinth*.
[30] Zielinski, *Deep Time of the Media*, 72 ff.
[31] Rosenheim, *The Cryptographic Imagination*, 202.

The digital form of steganography is still useful and surprisingly popular today, although I argue it should be understood as functionally and ontologically distinct from cryptography. Whereas cryptography is defined by its very special identity requirements (see chapter five), steganography is limited only by its user's imagination and willingness. Unlike cryptography, steganography is fundamentally obfuscatory in a mimetic, or illusory way.[32] For example, if one were to inflate a balloon, write a message on it and then deflate it, the message would be obfuscated and therefore useful for secret communication. In this example, the message itself is not altered in any "analytical" sense; the message is simply shrunken down so that it cannot be easily read. Even in the case of digital steganography, which might *also* include a cryptographic component, its fundamental operation is to "hide" the message, not to alter the message itself, and therefore (as per my analysis below), it is not a form of cryptography.

All computerized forms of cryptography use algorithms to accomplish their task, but the basic idea is actually an ancient feature of cryptography, and was first explored well before the invention of computers. In fact, cryptography was long used as a form of computational thinking, analysis, and investigation (sometimes even in the specific context of a "science"), dating back to the early history of cryptography. The etymology of the term "algorithm" reveals this connection: in its earliest use, "algorithme" referred to "the art of reckoning by Cyphers."[33] Following this trace further, the roots of "reckon" are "to make orderly"—that is, orderly thinking and production through the use of an algorithm. As I discuss in chapters three and four, this proto-history of algorithmic thinking stems from Raymund Lull's cabalistic combinations of natural symbols in the thirteenth century, which, through a chain of influences, were adapted by Leon Battista Alberti for his invention of polyalphabetic enciphering disks.[34]

Cryptanalysis, "code breaking," or "cracking," is often regarded as decryption without a key, or decryption by unauthorized means, but this is not quite right. As I explain in detail in chapter nine, cryptanalysis is ontologically distinct from decryption. Cryptanalysis may have the outward appearance of decryption, and may even end up producing the original plaintext, but the difference is that cryptanalysis is not the *deterministic* reversal of encryption. This is an important

[32] For a description and analysis of the range of ways that obfuscation can be used today, which includes steganography, see Brunton and Nissenbaum, *Obfuscation*. In chapter three I discuss the challenges of interpreting coded technologies in terms of mimesis.
[33] "Algorithm, N."
[34] Kahn, "On the Origin of Polyalphabetic Substitution."

distinction. Unlike decryption, cryptanalysis works by making an educated "guess" about the composition of the encryption algorithm and/or the original plaintext, but even when such guesses are backed by statistical rigour that overwhelming recommends a particular result (as with "scientific" cryptanalysis), the result is still a guess. Decryption, unlike cryptanalysis, works in strict accordance to the original plaintext-to-ciphertext "semantics" of encryption,[35] and is as guaranteed and certain as the original instance of encryption.

The *locus classicus* of the history of cryptography is David Kahn's *The Codebreakers* (1967), which summarizes the accepted terminology and conceptual distinctions in use today, he writes, "Cryptology is the science that embraces cryptography and cryptanalysis."[36] Alongside Shannon's exploration, Kahn's definitions and rich historical descriptions were deeply influential to historians and practitioners of cryptography alike,[37] helping advance the contemporary understanding of cryptography as a combinatory method of substitution and transposition from one alphabet into another. Correspondingly, through the twentieth century, steganography was no longer considered a variant of cryptography, but rather, seen as a completely separate form of hidden or invisible writing. Oddly, however, due to the historiographical focus and real practicality of military applications of cryptanalysis, the study and application of cryptanalysis was elevated to a sister field of cryptography, under the banner of the broader category of cryptology. But, as I will make clear throughout this dissertation, there is good reason to focus our attention on cryptography alone—as a form of writing, and outside of the scope of military applications—which therefore problematizes the dominant contemporary understanding of the field, and its application, techniques, and tools.

1.2 Ways of understanding cryptography

All of the philological complexity present from antiquity to early modernity eventually gave way to a powerful form of instrumental rationality in the mid-nineteenth and twentieth centuries. Instrumental rationality, or instrumentalism, is the belief that technology is only/primarily a "means" and a

[35] As I describe below, in my unusual usage of the term, the "semantics" of encryption are *not* the message's meaning (as it relates to human interpretation). Rather, the semantics of encryption are the links between plaintext and ciphertext.
[36] Kahn, *The Codebreakers*.
[37] Diffie and Landau, *Privacy on the Line*.

human activity.[38] That is, as a means and human activity, technology is a "contrivance" that conditions our relationship to it.[39] According to Martin Heidegger, instrumentalism is a worrisome general feature of late modern thinking, and not just because it fails to capture the essence of technology (Heidegger argues that technology's essence is "nothing technological"). Heidegger worries that by falsely conditioning our relationship to technology, we will turn our surroundings into "standing reserve," seeing the world as merely the raw material for human exploitation. Because humans are fundamentally technical creatures, we therefore run the risk of turning each other into standing reserve, to be used as raw material.

Oddly, proponents of instrumentalism believe that they sidestep politics altogether, since technology is assumed to be neutral to the variety of ends it can be employed to achieve.[40] According to the instrumentalist view, technology does not carry normative weight; a hammer is just a hammer, as a gun is just a gun. Norms, instrumentalists argue, are a result of human use—as the famous phrase goes, "guns don't kill people, people kill people." Similarly, instrumentalism views technology as universally applicable, since given any possible situation, if the technology is compatible, it is (and ought to be) applicable. An instrumentalist, one might imagine, sees no difference in employing cryptography for safekeeping government secrets, Facebook chats, or child pornography. Instrumentalists might argue, at best, government or personal interests dictate the application of cryptography; at worst, the application of cryptography is the result of business decisions from Silicon Valley foisted on consumers.[41] Either way, on this view, decisions are not based on values essential to, or constitutive of, the technology itself.[42]

A similar kind of thought, coined "solutionism" by Morozov, also lies behind much thinking about cryptography.[43] Morozov critiques the dominant values of Silicon Valley thinking by arguing that solutionism presumes rather than

---

[38] Heidegger, "The Question Concerning Technology."
[39] Feenberg, *Questioning Technology*.
[40] Feenberg, *Transforming Technology*.
[41] DuPont, "Opinion: Why Apple Isn't Acting in the Public's Interest."
[42] The conventional alternative to instrumentalism is substantivism, the view espoused by Heidegger, according to Feenberg, (*Critical Theory of Technology*). While this view has somewhat more merit than instrumentalism in my opinion, it too has serious problems, especially when paired with a common form of pessimism about technology's influence. For an in-depth analysis of the varieties of philosophy of technology see Feenberg's work, especially: *Critical Theory of Technology*; *Questioning Technology*; and *Transforming Technology*. I have no allegiance to any particular view of technology, rather I attempt to be sensitive to the insights of technologists, social scientists, and philosophers—spanning the range of potential positions.
[43] Morozov, *To Save Everything, Click Here*.

investigates the problems that it is trying to solve. Solutionism is not just the presupposition that there are easy technological fixes, nor the fact that some problems are not well suited to the kinds of fixes available to Silicon Valley. Rather, solutionists see problems in need of fixing when there may not be problems in the first place. For instance, while it is surely correct to think that the government surveillance overreach exposed by Snowden required intense assessment, is it really the "problem" we have been sold? And either way, some degree of surveillance is only a "problem" if absolute privacy is presupposed, which has *never* been a feature of social life.

Although instrumentalism is now the predominant view within the cryptography community, this view of cryptography actually came about slowly, as greater skill and knowledge of cryptography was gained over time. Between the American Civil War (1861-1865) and World War II (1939-1945), the instrumentalist view emerged within cryptography, as open communication technologies, requiring cryptographic protections, proved essential for effective command and control technologies.

First, telegraphy required coded and cryptographic communications to protect easily tapped lines. By the end of 1863, Union forces in the north had over five thousand miles of telegraph lines in operation, and sent over a million telegrams (an average of three thousand per day).[44] These communications coordinated troop movements and, importantly, rail transport. The expansion of telegraphy and its cryptographic application was also a global phenomenon. While the civil war was raging in the Americas, Britain was expanding its imperial reach using telegraphy, which included laying the first transatlantic submarine cable in 1858 (but Britain only succeeded in laying a *usable* cable later, in 1866).[45] In fact, due to early domination of global telegraphic communication, Britain held strategic signals intelligence until the end of the Second World War. Americans did not possess a transatlantic telegraph cable that did not pass through Britain until 1943.[46] These materialities, as they developed in this urgent historical trajectory, left little time or interest for alternative ways to think about cryptography.

Second, wireless radio communication required cryptographic protections to prevent enemy forces from eavesdropping, since signal interception was easy, even from afar. Given British dominance and its strategic position in telegraphy, by the 1890s there was considerable interest in producing an

[44] Giblett, *Sublime Communication Technologies*, 43.
[45] Hugill, *Global Communications since 1844*, 28.
[46] Ibid., 50.

alternative to submarine cables for international communication. During the first World War (1914-1918), America finally technically surpassed Britain's skill at wireless communication (given how far behind the Americans were in terms of wired communication technologies, wireless was considered essential research and development). Later, during the second World War, especially for the US military, wireless communication enabled rapid coordination of ground troops and supplies, and air-to-surface radar permitted night flying and bombing raids (including effective strikes on German U-boats, which had previously proven decisive in battle).[47] Through the two world wars, these wired and wireless technologies required robust and reliable cryptographical protections.

At the end of the second World War, and declassified immediately after, important mathematical theories for cryptography were developed by Claude Shannon, who ultimately led the field to further refinement of the instrumentalist view. Shannon sharply discriminated between two senses of "secret" writing: visibly hidden (steganography) and semantically "hidden" (cryptography). In his 1945 memorandum, "A Mathematical Theory of Cryptography," Shannon stipulated that "true secrecy systems" concealed the meaning of a message by cipher or code, which was an important distinction over earlier systems, that "confused" codes and cryptography.[48] Moreover, the idea of concealing *meaning,* and meaning alone, led to an important conceptual advancement, and later developed into theories of discrete encoding and information (realized in Shannon's *Mathematical Theory of Communication*).[49] This analytical work led Shannon to conclude that cryptography (and information) systems should be engineered using syntactic properties only. Meanwhile, over at Britain's Bletchley Park, Alan Turing's cryptanalysis efforts during the second World War helped refine similar themes, which, together with Shannon's work, led to the development of core theories of information and computing technologies.[50]

---

[47] Ibid., 146.

[48] Shannon, "A Mathematical Theory of Cryptography."

[49] Shannon and Weaver, "A Mathematical Theory of Communication." Shannon was far from the only person to suggest that "information" should be determined by syntax alone. Shannon got the idea from Hartley, who had been working on telegraph transmission; see Hartley, "Transmission of Information." During the Macy conferences, which Shannon participated in, this topic was vigorously debated, with engineers and philosophers arguing that a semantic view might be a more fruitful approach. See Cherry, "A History of the Theory of Information"; Thomsen, "Some Evidence Concerning the Genesis of Shannon's Information Theory."

[50] This history of information has been insufficiently studied with attention to the role of cryptography, but see Dyson, *Turing's Cathedral*; James A. Reeds, Whitfield Diffie, and J. V.

In an interview with Ellersick, Shannon described how his famous work on information theory stemmed from his work on cryptography.[51] In this interview, Shannon remarked that his development of the theory and mathematics for cryptography was in large part due to the immediate concerns of the Second World War. Shannon's conceptual innovations, however, might be more proximately located in prior work on "digital" information, as traced through the nineteenth and twentieth centuries, from Morse to Hartley and Nyquist.[52] Although the real-world *impact* of Shannon's contributions have in recent years been called into question (and any such history of Shannon information theory risks substantiating a "great men" view), Shannonian information did eventually become an essential part of daily life, and so too did cryptography, thereafter, on instrumentalist terms.

The work of Shannon, Turing, and others in this period of technical mastery and growing instrumentalism also helped characterize cryptography as mathematical. While mathematics have long played an important role in cryptology (see, e.g., the role of statistics in medieval Arabic cryptanalysis in chapter nine), during this period, considerable engineering advances were made possible by greater subject clarity and mathematical sophistication. These mathematical advances brought about further instrumentalism, and indeed, cryptographic exceptionalism. Until relatively recently, few scholars believed in the very sharp division between the mathematical world and the linguistic world,[53] just as until recently, few scholars believed in the sharp division between cryptography and writing. In fact, as I will argue below, the development of suitable notation, alongside notions of transposition and order—but *not mathematics*—dominated scholarly interest in cryptography for the vast majority of its history. Only by the time of Newton and Leibniz had questions of notation begun to settle, and subsequently, subject clarity and the

---

Field, *Breaking Teleprinter Ciphers at Bletchley Park*. Mackenzie's article on Turing's "On computable numbers" also offers a history and some theorization (Mackenzie, "Undecidability."

[51] Ellersick, "A Conversation with Claude Shannon").

[52] Hartley, "Transmission of Information"; Nyquist, "Certain Factors Affecting Telegraph Speed." See also Peirce's contributions, although they do not appear to have been influential (Beaulieu, "Peirce's Contribution to American Cryptography").

[53] This view is usually associated with non-Platonic conceptions of mathematics, which are uncommon and unpopular today. Rotman is one of the few trained mathematicians living today who has been effective in casting doubt on the special status of mathematics, although there has always been a fringe element within the mathematical community. In my opinion, the best expression of doubt remains Wigner's 1960 work on "The Unreasonable Effectiveness of Mathematics in the Natural Sciences," also later discussed by Kirby. See Rotman, *Mathematics as Sign*; Wigner, "The Unreasonable Effectiveness of Mathematics in the Natural Sciences"; Kirby, "Enumerating Language."

possibility of a mathematics of cryptography arose, which also caused notions of transposition and order to be subsumed under a new mathematical field of combinatorics.[54] Despite these radical changes (compare Leibniz's analysis of order in the seventeenth century to Bacon's in the sixteenth), mathematics did not suddenly become any more true, more foundational, or even better able to describe cryptography. In fact, even today, the "mathematics" used to produce encryption functions sits on top of deeper analytical properties, which I describe as notational. For these reasons, we should question the degree to which we focus on the mathematical properties of cryptography.

For instance, the invention of public-key (or asymmetric) cryptography in the 1970s by Diffie and Hellman has been heralded as a product of mathematics, but in fact, public key cryptography can be understood in terms of classical cryptography, and remains deeply indebted to it.[55] To see why, we must understand that there are two key ideas that differentiate public-key cryptography from its older private- (or symmetric-) key counterparts. The first is social—public key cryptography requires particular arrangements of individuals and institutions (in the most elaborate sense, this might amount to a large "public key infrastructure").[56] Such social arrangements are obviously not products of mathematics. The claim that public key cryptography is essentially mathematical, however, usually focuses on the key generation process that is necessary for the encryption algorithm, sometimes called "trap-door," "one way," or "knapsack" mathematical functions. These functions, which are *usually* mathematical, are easy to compute but hard to invert (typical mathematical problems used for this purpose are the discrete logarithm problem, and the difficulty of factoring integers that are the product of large primes, but other functions exist, such as newer ones based on elliptical curves). These problems are used to create a key with two parts (or a split key) that are linked in such a way that by using the one (public) key it is easy to encrypt but hard to decrypt, while the other (private) key can easily decrypt messages that have been encrypted by the public key. Special mathematical functions are used for key *generation*, that is, for the specific way the keys are linked (the actual encryption is typically a form of traditional encryption). To see why mathematical

[54] See Gardner, *Logic Machines and Diagrams*. Cryptanalysis has a separate history relating to mathematics, which I explore in chapter nine.

[55] This is a surprisingly controversial position to hold today, no doubt due to widespread belief in the powers of mathematics. Whitfield Diffie strongly disagreed with my characterization of public key cryptography in terms of classical cryptography, and not mathematics, when I posed the question to him.

[56] Blanchette, *Burdens of Proof*.

exceptionalism is problematic, it is worthwhile to investigate the lineage of these mathematical functions, as with William Stanley Jevons.

The trap-door function was first discussed by Jevons in 1874, although his contribution does not appear to have had any direct historical impact on Diffie and Hellman's later invention. Despite not having any historical impact on later developments, Jevons' analysis is important because it situates the trap door function within a broader category of being, outside of the special status afforded to numerical calculations. Anticipating the trap door function used in later public key cryptography, Jevons notes, "[t]here are many cases where we can easily and infallibly do a certain thing but may have much trouble in undoing it," and then points to the precise problem used in contemporary RSA encryption—the difficulty of factoring integers that are the product of large primes.[57] Jevons asks, "[c]an the reader say what two numbers multiplied together will produce the number 8,616,460,799?"[58] Remarkably, Jevons goes on to discuss how this problem applies to "the difficulty of decyphering [*sic*, i.e., cryptanalyzing] with that of cyphering [*sic*]."[59]

Despite this remarkable anticipation of later developments, however, it should be noted that far from creating a nineteenth century version of the RSA encryption protocol, Jevons is actually referring to the challenge of cryptanalysis, not decryption, which, as I will demonstrate in chapter nine, is a distinct process. Nonetheless, Jevons provides a useful historical lesson; his exploration of cryptography comes under the heading of "induction," which he argues is the *inverse* operation of deduction. That is, according to Jevons, logical problems also have the same property of one-way/trap-door functions. Jevons was also led to explore these issues in terms of combinations and permutations (again, like later cryptological developments), which led him to conclude,

> *Nor is this art or doctrine to be considered merely as a branch of the mathematical sciences. For it has a relation to almost every species of useful knowledge that the mind of man can be employed upon.*[60]

So, for Jevons, the trick to "trap-door" problems is a *general* one that has consequences for cryptography, but equally so for logic (he would later build a machine capable of computing syllogisms), and indeed, it is applicable to "every species of useful knowledge."

---

[57] See also Golomb, "On Factoring Jevons' Number."
[58] Jevons, *The Principles of Science*, vols. 1, 142.
[59] By "decyphering" Jevons means cryptanalysis, which he explains in the next sentence: "to decypher the letter having no key." Ibid., vols. 1, 143.
[60] Ibid., vols. 1, 199.

Exempting Jevons' explorations, which never directly influenced the history of cryptography, the challenge for modern public-key cryptography has always been to find suitable version of these special mathematical functions. When first developing the idea, Diffie asked Donald Knuth for suggestions for mathematical functions that might have the needed property—and in fact Knuth suggested the prime factorization problem (although Diffie did not use this for his system).[61]

Finding suitable trap-door functions remains an active area of research today. All known trap-door functions suffer from the not inconsiderable issue that they rely on a *lack* of knowledge about their workings, and not mathematical proofs. However, in recent years, quantum cryptography has emerged as a potential saviour, which dispenses with mathematical functions altogether, and instead uses physical (quantum) properties to create a similar kind of "trap-door" function.[62] Therefore, given that logical and quantum trap-door functions can in theory replace the mathematics used in public-key cryptography, I believe we should question the typical characterization that mathematics is essential to cryptography.

Traditional cryptography can just as easily rely on more basic principles, especially when it comes to encryption (rather than key generation). In fact, the most secure kind of cryptography—proven to be "perfect" and uncrackable—is the one-time pad, which requires nothing more than a random alphabet and the application of the logical properties of the "exclusive OR." Similarly, most contemporary encryption makes due with a variety of transposition and substitution transformations working on binary code (cf., "substitution boxes" used in symmetric key algorithms). But beneath the mathematical, logical, and quantum perambulations applied to cryptography lies its brute inscription in the world—as paper and pencil, magnetic flux on ferromagnetic material, or polarized photons. This inscription is often overlooked (as "mere" binary encoding), but as it turns out, it is of critical importance.

It is critically important to understand that cryptography must begin with plaintext, which is a specially prepared configuration of the world—sometimes expressed as representational symbols—that abide by the rules of notation. In cryptography, the plaintext notation is then transformed by encryption, resulting in ciphertext. These inscriptions change their syntax when encrypted, but must remain inscribed in a form of notation. I argue that we ought to

[61] Levy, *Crypto*, 83.

[62] Quantum cryptography uses quantum superpositions and entanglement, which are almost certainly *studied* by mathematics, but are real, physical properties.

recognize the importance of this special inscription for cryptography, against dominant views that focus on technology and mathematics.

In recognizing the importance of notational inscription, we also recognize the ways that cryptography can be productively understood as a form of writing, and therefore can draw on a whole host of different influences, which generate a range of social, political, and representational outcomes that we would do well to attend to. But, first, to really appreciate the writing of cryptography we must also adjust our understanding of the basics of writing.

It is necessary to put aside the traditional Aristotelian conception of writing, which believes that writing is a "sign of a sign," based solely on spoken words and their meaning. We might, instead, focus on the ways that writing is materially instantiated. Also, cryptography and its processes (encryption, decryption, cryptanalysis) can be understood as forms of code and encodings. Despite the fact that lay people often (misleadingly) call cryptography "code," cryptography is rarely discussed in serious academic terms as code. One of the central challenges to using the term code is that "code" is highly polysemic, which has only confused matters and dissuaded serious academic investigations away from an otherwise ready connection to writing. This reticence to engage in discussions of code has meant that the emerging fields of software and critical code studies (having emerged out of the humanistic disciplines) have so far paid very little attention to cryptography, despite the obvious importance of the topic.

This oversight by the field of software and critical code studies has occurred in spite of the fact that the intellectual "father" of the field was Friedrich Kittler, a man who saw clearly that cryptography was the *alpha* and *omega* of code, and therefore writing. In his article on "code" in *Software Studies: A Lexicon*, Kittler wrote, "codes *materialize* in processes of encryption" (my emphasis).[63] And on the last page of Kittler's triptych, *Gramophone, Film, Typewriter*, he delivered the epigraph for the present chapter (and leitmotif for this dissertation), writing: "literature… *ends* in cryptograms" (my emphasis).[64] Despite the numerous challenges Kittlerian philosophy poses, his work is essential to any humanistic study of cryptography, as he was one of the few authors of the twenty–first century that dared to approach the subject, while also avoiding the

[63] Kittler, "Code," 40. Despite the fact that Kittler's article was indeed in the field-defining *Software Studies* volume, no other scholars associated with the field have yet engaged this topic, or Kittler's treatment of it.

[64] Kittler, *Gramophone, Film, Typewriter*, 263. There are a few other authors in critical code studies and software studies that investigate the role of cryptography in broader social terms, and its relationship to code (see chapter six).

instrumentalist pull. For Kittler, like those in the Renaissance and early modernity, cryptography—as a topic, field, technology, and process—was a powerful force capable of reaching deep into human expression, thought, and being.

The polysemy of "code" can also be useful for drawing links between cryptography and other technologies. Cramer and Mackenzie have each explored the connections between cryptography and computer code. Cramer traces the development of code through a long historical path and concludes:

> *"[C]ode" not only refers to cryptographic codes, but to what makes up software, either as a source code in a high-level programming language or as compiled binary code[.]*

Mackenzie, for his part, argues that "computation is cryptographic." Computation, according to Mackenzie, is a "kind of depth or secrecy" characterized by "cryptographism."[65] As my analysis will show, there are in fact a great number of historical and philosophical connections between computing and cryptography. This includes the development of notation (and specifically, Bacon's introduction of binary), and mathematical and ordering machines (Leibniz's stepped reckoners), which arose in cryptographic contexts. However, while Mackenzie's analysis is novel, from my perspective it suffers from the belief that cryptography is primarily or only secret or veiled, and it fails to distinguish between cryptography and cryptanalysis. Despite these failings,[66] Mackenzie is perhaps the only modern author who has went as far as Kittler in attempting to align code or computation with cryptography.[67]

Scholars in humanistic and normative traditions would do well to start paying closer attention to cryptography, in general, and with respect to its numerous connections to writing, computation, and algorithmic technologies.[68] Over the

---

[65] Mackenzie, "Undecidability," 369.

[66] Mackenzie's interpretation of Turing's work on "computable numbers" also confuses a number of issues, as explained to me by Brian Cantwell Smith. For example, Mackenzie overplays the "undecidability" of systems of marks and its relationship to the famous "halting problem."

[67] With Bradley Fidler, I have also recently demonstrated the close historical interactions between computation and cryptography, from a history of network technologies; see DuPont and Fidler, "Edge Cryptography and the Co-Development of Computer Networks and Cybersecurity."

[68] There are a significant number of scholars studying the normative aspects of cryptography (really, cybersecurity) from a legal and policy standpoint (e.g., Nissenbaum, "Privacy as Contextual Integrity."), but these authors never seem to properly question their unit of study. Similarly, scholars studying the socio-political aspects of cryptography have tackled normative questions (e.g., Deibert, *Black Code.*), but like the legal and policy scholars, they do not

last twenty years, from the crypto war of the early 1990s to the Snowden leaks (2013-), there has emerged a palpable sense of politics around the use of cryptography. Back in the 1990s, the cypherpunks clearly won the crypto war: cryptography was removed from the munitions list, the terms of collaboration with government for standards development were largely dictated by industry, and strong cryptography was deployed globally. As later revealed by the Snowden leaks, government responses to the original crypto war were to systematically circumvent, infiltrate, disable, or crack cryptographic protections, re-enabling broad surveillance powers. More recently, since the Snowden leaks, once again, many of the routes governments used for bypassing or cracking cryptography, post-1990, have again been closed by more diligent and sophisticated applications of cryptography. Sensing still further challenges to their ability to bypass and crack cryptography, governments have returned to rhetoric used during the crypto wars of the early 1990s, claiming that law and order are at jeopardy if strong cryptography is deployed widely and disables legal surveillance. The usual bogeymen have become a political pitch: cryptography allows terrorists, drug dealers, and child pornographers to operate and communicate freely. At one point, UK Prime Minister David Cameron collaborated with US President Barak Obama on the issue, seeking a unified political front that would force companies to put "back doors" into the cryptography that has been deployed so widely in recent years. Cameron even asked rhetorically, "[a]re we going to allow a means of communications which it simply isn't possible to read?"[69]

Perhaps as a result of the lack attention placed on cryptography, politics of cryptography by the humanities (its use, regulation, and development) seems to be at a standstill. Government and law enforcement agencies believe that strong cryptography will lead to disorder and lawlessness. But governments clearly have vested interests in controlling populations, which relies on surveillance capabilities. Concerned citizens and technologists believe that strong cryptography provides much needed privacy and freedom of speech. But there is a risk of going too far towards some imagined utopia, and either way, citizens rarely have a hand in the production of cryptographic technologies, and usually act only in their capacity as consumers, subject to the will and whim of technology companies.[70] Much of the standstill results from the ostensible

problematize the status of cryptography (it is either, and only, strong or weak, regulated or not, consumer or state, open or closed, and so on).

[69] Hope, "Spies Should Be Able to Monitor All Online Messaging, Says David Cameron."

[70] DuPont, "Opinion: Why Apple Isn't Acting in the Public's Interest."

totality of the positions: according to technologists, weak cryptography is no cryptography at all, so either messages are completely private or not at all. In the current climate of discourse, it is not clear how this standstill will be resolved. And the matter will only become more acute as we learn how to more reliably deploy strong cryptography, and deploy it ever more widely.

So, how do we make progress on these pressing issues? I propose that we draw lessons from the archeology of cryptography. Doing so will draw the study of cryptography into comparison with writing, computing and media technologies, and away from views that reduce it to mathematical features or technological parts. Writing an archeology of cryptography requires a focus on the disjunctures, gaps, and breaks within and across historical epochs, and it must also recognize that cryptography is a profoundly technical apparatus (this does not, however, imply that we should study cryptography *as* technology).[71] That is, these lessons are to be drawn from the *conditions of possibility* and a *technical a priori*. Such an analysis reveals a diverse history for cryptography, cutting across the development of artificial language, machine translation, media, code, notation, silence, and order.

[71] Cf. Foucault, *The Archaeology of Knowledge*; Agamben, *"What Is an Apparatus?*

2
Rewriting cryptography

In this dissertation, "cryptography" is my intelligible unit of study. I argue that cryptography is, at least traditionally, a technical form of writing, and more recently, a computing technology and transmission medium. My method for understanding cryptography is to look at it archeologically, in a roughly Foucauldian sense, which has been revised to attend to technical artifacts.

This methodological revision follows the insights of the last few decades of media theory (particularly "German" media theory). I do not adopt the approach of media theory because cryptography can only be explained in these terms (however, media effects are particularly important, especially with respect to the encryption transformation, as discussed in chapter seven). Rather, media archeology offers an approach that permits understanding the technological aspects of cryptography, without treating it *as* technology. In this chapter, I analyze media archeology in terms of what I believe are the method's constituent parts: a roughly Kantian and Foucauldian exploration of the conditions of possibility, and an analysis of the technical a priori. My analysis of the conditions of possibility of cryptography, as befits the method, is largely historical. My investigation of technical a priori, on the other hand, requires recognizing that technology is an "event," a rupture of temporal sequences that otherwise excludes or leaves invisible important agents (here referencing the literature on "event," most famously aligned with the work of Badiou). As an event, cryptographic technology registers reality in advance of meaning. Being an invisible or excluded agent, the a priori of cryptography emerges as epochs (specific realities for specific eras), and is not ahistorical or panhistorical (as "a priori" might otherwise sometimes imply, especially in analytical philosophy).

The conditions of possibility are necessarily historical, and as such, histories of cryptography dominate the present study. In this chapter, I present one possible characterization of the technical a priori for cryptography, that is, mapped as the technical conditions of possibility that permit the existence or emergence of cryptography in a given context. Put another way, technical a priori is a description of interconnections through local analysis, while the conditions of possibility describe the global limitations, but also the necessary framework for cryptography to emerge in any given context.

As I described in the previous chapter, my goal is to complicate the instrumentalist picture we have inherited, to better understand how we think

about cryptography, as a field, mode of technology technology, process, and way of being. I reject the contemporary view that cryptography should be understood *as* technology for two reasons. First, the picture is too simple and necessarily biased towards the present moment; throughout its history, cryptography has not always been understood as a technology. Indeed, this is almost tautologically true, since the concept of technology is itself a relatively new invention.[1] By looking at the history of cryptography in use—what the scholars and inventors thought they were doing, and what they believed to be true—the picture becomes complicated by the many heterodox and heteroclite uses of cryptography. In the past, more often than not, scholars thought of cryptography as a form of writing within the liberal arts, and not as a mechanical art.

Second, this picture of cryptography as technology is insufficiently clear. That the lack of clarity has not stemmed the speed of industrial research and development, today, is a small miracle owing to the power of technological abstractions, but it also obscures the tremendous amount of intellectual work that has gone into *creating* a suitably simple and stable black box capable of supporting myriad uses. Indeed, most of this hard work of abstraction has occurred in the last one hundred years, driving an agenda of instrumentalism, and correspondingly leading to significant technological invention. My goal in this dissertation is to open the black box and let the complexities run amok, and see if some coherent semblance of an intelligible unit of study emerges.

Unlike most work on cryptography, the present study very consciously excludes extended descriptions of the technical workings of cryptological systems, and for the most part shies away from historical events from the last century. Of course, cryptological systems and methods are sometimes described, in general ways, but technological descriptions do not drive the narrative. In the mainstream study of cryptography, this is a surprisingly unorthodox approach, even though most contemporary studies of technology, ranging from science and technology studies, to media studies, to sociological studies of technology, long ago dispensed with such technologically-determinist, Whiggish

[1] The issue of the status of "technology" in history is complicated and unsettled. In recent years historians of science and technology have re-evaluated the status of labour and crafts in antiquity and the middle ages, suggesting closer than previously thought connections between the rarefied subjects (science and liberal arts, inherited from the Greeks) and the base ones (mechanical and technical arts). It is now generally accepted that through the middle ages there was considerable cross-pollination between liberal and mechanical arts; see Whitney, "Paradise Restored. The Mechanical Arts from Antiquity through the Thirteenth Century." The present study implicitly corroborates these newer views of the history of technology, offering evidence of the fluidity between writing practices, science, and the invention of mechanical devices.

approaches, which still dominate the study of cryptography. This unorthodox approach is key to my method and goals, which attempts to expand and problematize the ways that cryptography has been thought about.

In this study, I attempt to understand what sets of beliefs, what actions, and what configurations of social, political, and personal relationships must exist for such a technology to arise—that is, to investigate its *discourses*. One of the consequences of this approach is that technological artifacts without well-developed discourses are underrepresented. Unlike material archeology, for instance, which might be interested in how a clothes pin reconfigured life within a village in medieval Africa, this (discourse-centric) archeology lacks tools to meaningfully make sense of these kinds of stories.

Moreover, throughout this dissertation there is an alarming lack of engagement with non-Western thought and technologies. Some attention is given to the medieval Arabic contributions (chapter nine), but none is given to Asian peoples, who surely had the need (and actual technology?) for cryptography. Admittedly, part of the reason for the lacunae is the lack of available resources and the significant challenges of reading and understanding non-Western languages. But for sure, part of the reason for the lacunae is a methodological blindness to the integration of such empirical realities (still today, it is basically unknown whether the mighty Chinese empires *even had* cryptography).[2] Every method has its zones of insight and blindness, and this is mine.

Although the issue and topic of representation is frequently explored throughout this dissertation ("what are written symbols if not representational?" one might ask), this does not imply that cryptography was always understood as representational, or understood as representational in familiar ways. For example, scholars working on cryptography and its cognates from the sixteenth to the eighteenth centuries thought that cryptography was representational, but not as we might expect. Curiously, these scholars thought of plaintext as representational in the sense that they believed it to be part of ciphertext, in ways foreign to today's thought. As I discuss in chapter four, in an unusual twist, scientists were trained to interpret ciphertext in nature, which presupposes a world as occult and coded and therefore representational in *hidden* ways. Other times, however, representation worked very differently, or

[2] For a discussion of the benefits of more seriously *empirical* historiography of technology, and one plausible approach for redress, see Edgerton, *The Shock of the Old*. Edgerton avoids instrumentalism on account of his ability to reframe the subject of historiography of technology; he writes: "[historiography] become[s] much easier… if we stop thinking about 'technology,' but instead think about 'things'."

not at all. For instance, in chapter five I discuss the "discourse network 1900," which imagined earlier and more representational eras to have suffered from illusion. By 1900, "universal alphabetization" transformed writing into a process of "selection" from a "countable, finite supply." Interpretation, usually a critical component of representation, was therefore rejected as a viable means. Then, in chapter eleven, I discuss the ancient Spartans' use of cryptography and find an entirely different and rather foreign set of determinates and functions. In fact, the Spartan use of cryptography counters the prevailing narrative that cryptography is only, or primarily, used for secrecy. Rather than engage the concept of secrecy—the representational strategy of hiding meaning—the Spartans made use of cryptographic technology to function for their well-known affinity for silence, which I argue helps us understand how cryptography might have worked in their society, yet, is unlike how either silence or cryptography is thought to work today.

Beyond these histories, I argue that cryptographic apparatuses register reality prior to human meaning making. Indeed, this is as much a historical fact as it is a technological one, and marks the point where my method diverges from the strict archeological method. In a similar way, following Badiou, Mackenzie describes technology as an "event," to indicate the ways in which it "is not completely reducible to historical understanding."[3] In the present study, I attempt to walk the fine line between purely historical determinations that recognize how functions and meanings—what Foucault called positivities—are essentially part of their specific historical epoch, and the ways that technological artifacts have a certain kind of empirical and analytical, and therefore independent reality. The former—positivities such as "science," "secrecy," and "language"—are dependent upon a grid of reality that has internal coherence and a set of *conditions of possibility*. The latter, the technological artifacts in use, depends equally on the positivities and the conditions of possibility as it does on certain analytical and empirical realities, such as physical properties of the universe, mathematical truths, and logical laws—investigated as *technical a priori*.

In the context of meaning making, following Foucault, "Man" the knower is destabilized by cryptography. Indeed, this erasure of hermeneutical "Man" is precisely why, in chapter eight, I turn to mythical *angels* as transmission media. Angels work to metaphorically ferry "meaning" between plaintext and ciphertext, a function that is otherwise an impossibility for a knowing person. And so, the traditional, hermeneutical story that encryption is a human activity,

[3] Mackenzie, "Undecidability."

revolving around specific human needs and desires, needs revision. The diverse functions of cryptography—science, communication, secrecy, mathematics, liturgy, and so on—are the *result* (not *origin*) of cryptography. These functions arise from the positivities, grids, and schemas underlying human experiences.

Despite drawing from realities largely inaccessible to human thought—that is, the necessity of angelic transmission and the destabilization of "Man" the knower—the development of cryptography is not independent of human involvement. Rather, cryptography *requires* a great deal of effort and infrastructure to sustain its existence. But ultimately, we design tools *against* our own understanding—since, obviously, we cannot interpret the resulting ciphertext. The social consequences of building tools against our own understanding is ongoing, the dynamics of which have reached a feverish pitch today, as cryptography infiltrates more aspects of modern life, and leads to crisis.

What, then, does cryptography mean for our late modern, late capitalist, digitally interconnected lives—our *épistème*? While cryptography has thousands of years of history, given its outsized role in contemporary life (evidenced by Snowden's revelations), what does it mean for cryptography to mediate and remediate so many communications? If cryptography is now an essential part of media, do we still have the intellectual tools to understand media? What would such tools look like? What should we make of the mediatic connection between plaintext and ciphertext? What binds the identities that form between plaintext and ciphertext—the medium we conventionally call "encryption"?

Unlike broadcast media, which function specularly by reflecting human thoughts and desires, cryptography works through invisible forces of transformation and order. But does cryptography help to reveal or obscure the digital world? Or, perhaps, thinking rather orthogonally from our typical narrative, does it order? Communicate? The pressing technical questions that arise from this line of heterodox line of thinking might be: what are the relationships between cryptography and search engines, logistics algorithms, financial information technologies, Internet switches and routers? Or, what relationships do the many encryption algorithms have to big data, analytics, and surveillance? Most pressingly, have we asked sufficiently deep questions about state secrecy and "privacy enhancing" consumer-level cryptographic countermeasures? Is the latter perhaps just more of the former? How important

is it to understand cryptography, and what intellectual tools do we use, given that we live in a "network society"?[4] "Infosphere"?[5] "Black box society"?[6]

As any tool of communication and expression gets taken up in society, our ways of communication and modes of organizing the world change. Sometimes these tools augment, diminish, or revolutionize our abilities. The traditional list of communications "revolutions" includes writing, the printing press, and the computer—but others could be included, such as paper making, double-entry bookkeeping, telegraph, radio, television, and perhaps—cryptography? If we recognize the impact cryptography is having on contemporary life, saying nothing of the past, does it prompt us to reconsider the ways that our relationship to language, writing, and other technologies is mediated? What is the impact on thought itself when writing is encrypted as a matter of routine?

These questions, and myriad others, probe the status of cryptography in our lives and the lives our predecessors (and future generations, no doubt). These are also political questions, or at least, are issues that frame the way that political questions get asked.

2.1 Conditions of possibility

This work traces an "archeology" of cryptography by identifying its conditions of possibility. Such conditions of possibility are fundamentally historical: as descriptions of the limitations of thought and being; the narrativisation of multiple pathways with their divergences, gaps, ruptures, and failures; and, the ways that epochal and contingent histories are delimited. Moreover, this archeology is "critical" in both senses of the word. As I described above, I am critical of the dominant view of cryptography and its widespread use, which I worry is causing unseen changes in the fabric of communication, expression, and sociality. I am also critical in the methodological sense introduced by Immanuel Kant, and later, Michel Foucault.

Writing in the context of Enlightenment thinking, Kant sought to reconcile modern (empirical) science with a priori understanding, and called his approach a "critique." The perceptual world, according to Kant, was an "appearance," and so, not independent of our intuition. But, in order to ground appearances, Kant required a method to discover the foundations and limits of experience. Kant found this method in his transcendental idealism, which supposed that space

[4] Castells, *The Rise of the Network Society*.
[5] Floridi, *The 4th Revolution*.
[6] Pasquale, *The Black Box Society*.

and time are formal features of our perception, not things in themselves. As a result, Kant denied that we can know that objects exist in space, a limitation due to our conditions of possibility. Foucault's project was Kantian in this sense of being "critical," but his solution avoided appealing to transcendental idealism. Instead, Foucault sought to understand axes of power and knowledge as the limiting conditions of possibility.

As Kant described in his *Critique of Pure Reason*, conditions of possibility are the necessary framework or schema that permits the possible appearance of something.[7] This schema sets the limits of reason, that is, the extent to which we can know the existence of some thing or to give it some meaning. In Kant's configuration, the essence/appearance distinction disappears, leaving just an apparition—that which appears, nothing more.[8] The transcendental limits of reason are a positive product of the self-referential nature of the appearance of being; that is, the knowing subject is constitutive of her own limits of knowing.

Foucault does not appeal to transcendental idealism to explain sense experience, as Kant had. Foucault described the historical a priori as a method to "rediscover on what basis knowledge and theory became possible," that is, as a way to "bring to light… the epistemological field."[9] Even though the historical a priori cannot be experienced directly, Foucault described it as the "experience of order" by which "knowledge was constituted."[10] In fact, the historical a priori is something of a paradoxical concept, in the sense that, for Foucault, each historical era and its archeological "stratum" has a distinctive epistemological structure, yet we apparently have (limited) epistemological access to these histories. Foucault argues, like Kant before him, that some structures (perhaps not transcendental ones) enable our critical epistemology.

This method investigates the ways that knowledge is constituted, order is experienced, and theory made possible. These histories are also sometimes disorienting and strange precisely because they do not serve the same master of traditional history. Indeed, as will become clear, cryptography has multiple origins and pathways, which include a surprisingly diverse range of things—thinking and logic machines, universal and perfect languages, music and dance notation, poetry and language, mechanical translation, memory devices, architecture, and algorithms. Many of these projects failed—universal language planning being the most famous—but by gaining some appreciation for why

[7] Kant, *Critique of Pure Reason*.
[8] Deleuze, "Kant, Synthesis and Time."
[9] Ibid., xxiii. For a critical investigation of Foucault's discussion of the historical a priori, see Han, *Foucault's Critical Project*, 38.
[10] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, xxii.

they failed (and comprehending their critical limits), we are better equipped to understand the inherent logics and schemas at play. The goal here is not to erase disjunctures and juxtapositions, or to explain them away as part of a larger narrative of continuity or progress, but rather to highlight their operative logics, their relationships, and their conditions of possibility.

But, where Foucault was largely silent on specific technologies, my entire dissertation is on the emergence of one particular "technology." This methodological issue is addressed in so-called German media theory, sometimes known as media archeology, which draws on Foucault's archeological method for investigating technology.[11] The dominant figure of German media theory, and strong defender of the Foucauldian method, is Friedrich Kittler. Similarly, Ernst, Siegert, Parikka, and perhaps Zielinski (among others), can be interpreted as espousing a form of "media archeology," a form of media theory that concentrates on understanding the conditions of possibility of technology. Indeed, the difference between German media theory and Foucauldian thought is less that of method than of topic. Somewhat oversimplifying matters, German media theory was deeply influenced by Foucault's method, but sought to explore technological materialities rather than knowledge and power.

It is also worth noting that a parallel tradition can be found in the work of Agre, who expands on Kant's articulation with his notion of "critical technical practice," which is an "expanded understanding of the conditions and goals of technical work."[12] And like Foucault's reimagination of Kantian critical philosophy, Agre calls for a "historically specific practice."

2.2 Technical a priori

While there is no singular method to media archeology, most media archeology is fundamentally interested in understanding the emergence of technologies. This is certainly true for Wolfgang Ernst. In his introduction to Ernst's *Digital Memory and the Archive,* Parikka describes a "wider academic debate" having to do with understanding current digital culture through a technological lens. While this goal is realized through diverse approaches, Ernst and other authors, according to Parikka, maintain "an enthusiasm for… objects."[13] Indeed, in attempting to offer an "insight into the a priori of historical writing," Parikka

[11] There is a great deal of debate as to whether there is a uniquely "German" field of media studies, but for sake of convenience I will adopt the denotation.
[12] Agre, *Computation and Human Experience*, 32.
[13] Ernst, *Digital Memory and the Archive*, 12.

expresses worry that these authors are "in danger of mythologizing the machine."[14] Others have accused the tradition, especially in its relationship to Kittler, as techno-determinist. Understood charitably, one might say that by drawing attention to the machine, the view of technology associated with media archeology is an expression of the post-humanism of digital culture. These posthumanistic origins, according to Siegert, are to be found in Foucault's "historical a priori," which "turned it into a 'technical a priori' by referring the Foucaldian 'archive' to media technologies."[15] Therefore, while still very much interested in actual technologies, media archeology is not so much techno-determinist, as a method for recognizing that technology can and does *condition* our *specific* experiences.

As Siegert describes it, the notion of a technical a priori developed within the context of German media theory, or media archeology, and was a unique expansion of the field of "cultural technologies," from the Foucauldian idea of a historical a priori. These authors rejected any discussions of "big explanatory models of a history of ideas of a philosophy of history."[16] In Britain and North America, on the other hand, media scholars, sociologists, philosophers, and historians focused, traditionally, on themes of progress, historical synthesis, freedom, and revolution. Communication studies, often allied with media studies outside of Germany, was predominantly concerned with what was represented *in* the media, not *how* it was represented.[17] As Siegert describes it, "the whole question of representation was shifted towards the question of the conditions of representation."[18] And so, in German media theory, sharp focus was placed on the materialities and infrastructures that enabled discourse networks within the foundation and limits of knowledge (the Foucaldian "conditions of possibility").

2.2.1 Mapping the technical a priori of cryptography

In the following section I offer one possible characterization of the technical a priori for cryptography, that is, the technical conditions of possibility that permit the existence of cryptography in a given context.[19] I contrast my characterization against two other mappings, one constructed from Kahn's

[14] Ibid., 10.
[15] Siegert, "The Map Is the Territory," 12.
[16] Ibid., 14.
[17] Ibid., 15.
[18] Ibid., 13.
[19] Or, in a somewhat too positivistic framing, what follows can be understood as a map of the "minimal" set of conditions—the raw materials—needed to realize cryptography in the material world.

influential 1967 *Codebreakers*, and the other from Zielinski's 2002 (2008 English translation) *Deep Time of the Media*.[20] Despite using very different approaches for very different ends, Kahn and Zielinski offer representative views of cryptography, and are of the few authors to provide a description and analysis as to how they think the parts of cryptography fit together. Of course, the comparison is loose because these authors had different goals than my own, conceiving of the issues in terms of domains of expertise ('what kinds of people and resources are leveraged for each domain'), rather than a priori, as I do. Furthermore, these mappings do not contain the same level of detail as my mapping. But, despite these differences of purpose and detail, the contrast is readily apparent, and offers a useful foil to better describe my characterization of the technical a priori of cryptography.

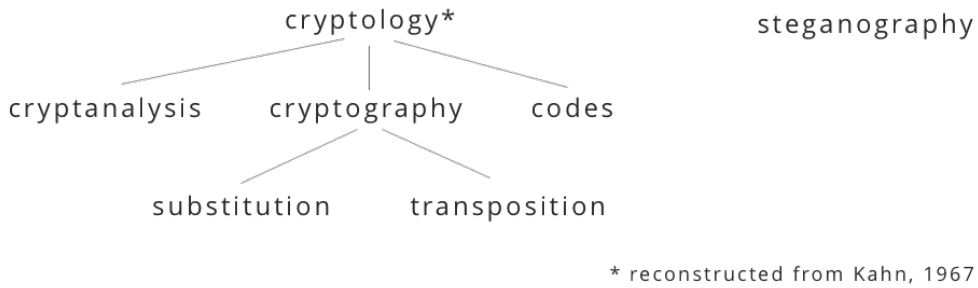


Figure 2.1: Construction of mapping of domains of cryptography, from Kahn's *Codebreakers*.[21]

In figure 2.1, I have constructed a mapping of the domains of cryptography from Kahn's *Codebreakers*. This diagram suggests that cryptology and steganography are separate domains, although the terms were never so clearly divided in history (and therefore, Kahn might resist such a depiction of his work). "Cryptology" writes Kahn, "is the science that embraces cryptography and cryptanalysis," which is reflected in the diagram as one of the central divisions. Outside of the study of cryptology lies steganography, a method to "conceal the very existence of the message."[22] Cryptography is a method to create "secret" messages by rendering them "unintelligible to outsiders," either through substitution and transposition (cryptography) or codes (which are typically whole-word substitutions, sometimes called "nomenclators").[23] In

[20] Kahn, *The Codebreakers*; Zielinski, *Deep Time of the Media*.
[21] Kahn, *The Codebreakers*.
[22] Ibid., xi.
[23] Ibid.

practice, there is often no clear line between cryptography and codes, but Kahn seems to want to reserve the prior for those that adhere to the "two basic transformations" of transposition and substitution. Cryptanalysis, on the other hand, is the process of breaking down or solving cryptography by "persons who do not possess the key or system."[24] Kahn never clearly explains what cryptography is "made" of, but he considers the range of historical cases, including letters, numerals, binary, and the many material substrata.

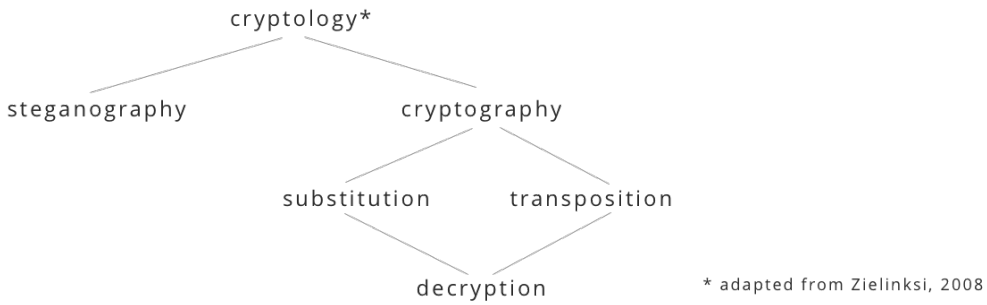


Figure 2.2: Redrawn map of domains of cryptography, from Zielinski's *Deep Time of the Media*.[25]

Zielinski's characterization is very similar to Kahn's, with the exception that he clearly understands steganography to be a central component of cryptology (Figure 2.2; the diagram is redrawn from its original, in *Deep Time of the Media*). For Zielinski, cryptology grew out of the "gradual separation of the message from the body of the messenger," which was a useful way to speed up transmission and prevent the messenger from gaining knowledge of the message's contents.[26] Decryption is diagrammed opposite from cryptography, which Zielinski appears to take to be the identical but reverse process of encryption.

[24] Ibid., xv.
[25] Zielinski, *Deep Time of the Media*.
[26] Ibid., 72.

Figure 2.3: My mapping of the domains, positivities, and technical a priori of cryptography.

My characterization divides natural language and cryptography, turning on a distinction between two kinds of semantics. Like Kahn, I place steganography in its own category of meaning, which I believe is a mimetic form of human expression, and thus associated with visual or imagistic arts and their mimetic forms of representation. In chapter three I offer an in-depth discussion of mimesis, and argue that methods that focus on mimetic qualities (often found in media studies) fail to capture the essential aspects of cryptography—mimetic methods that I here diagram as distinct from both cryptanalysis and cryptography. Unlike the characterization offered by Kahn and Zielinski, however, I argue that cryptanalysis is essentially linguistic, in that it operates on important aspects of language (such as message semantics, but also phonetic and morphological properties). As described in chapter nine, the core of the cryptanalysts' job is to understand how language works, and (for "scientific" cryptanalysis) to possess the ability to manipulate it through probabilistic measures. In this way, the cryptanalyst is a kind of translator, and draws extensively on *those* intellectual assets, quite distinct from the cryptographer. Cryptography, on the other hand, involves a set of transformational processes—encryption and decryption—that are a special kind of writing called "notation." Encryption, and its reverse, decryption,[27] are reflexively "semantic," through deterministic transformations of substitution and transposition (also called trans*cription*, which is distinct from the intentional semantic manipulations of trans*lation*).

Critically, my description of the technical a priori of cryptography focuses on the role of notation.[28] Indeed, every aspect of cryptography must remain notational, at all times, no matter the transformation that occurs, in order to remain associated with the class of expressions we call "cryptography." Whether understood in terms of semantic violence or syntactic change, from plaintext through encryption to ciphertext, and back again, all parts and processes must remain notational in order to count as cryptographic.

In the diagram, I include the simplified example of encryption inherited from Alberti, who writes, "[t]hus a common letter, say A, will take on the *meaning* of another letter, say G… [my emphasis]."[29] This seemingly simple transformation, from the mark <a> to the mark <g> encloses a number of complicated aspects. First, the <a> of plaintext must be notational (see chapter five), which (roughly

[27] I will generally use "encryption" to stand in for encryption and decryption, which I see as inverted correlates.
[28] See chapter five for a detailed analysis of the analytical requirements for notation.
[29] Alberti, "De Componendis Cifris."

speaking) means it must be discrete, and, the particular way the mark is expressed does not matter so long as it complies with the stipulated set of notational marks (e.g., that there is no relevant distinction between the marks <a> and <A>). Second, for encryption, the relationship between <a> and <g> is *transitive* or *indexical* in the sense that <a> is *reflexively* linked through an indexically "semantic" connection to <g>. In other words, in terms of the encryption substitution, <a> actually *means* <g>, but it does so, on my interpretation, in an unusual way.

Unlike most kinds of writing, which attempt to "reach out" to the real world (we usually call this "representation"), the semantic link that holds between plaintext and ciphertext in encryption looks "inwards" to its own set of marks (that exist in a larger combinatorial space). This is an unusual quality of encryption, which I believe requires an unusual sense of semantics. Because of this tight link between plaintext and ciphertext, through the process of encryption, the transitive and reflexive connection can never be forgotten or erased, or else decryption becomes impossible. Indeed, once the transitive link <a>→<g> is severed, the only way to return, from <a>←<g>, is by "guessing" the semantic link—in other words, the process of cryptanalysis, either through quasi-linguistic probabilistic measures, or the whole range of tools provided by linguistics (see chapter nine for a further description of cryptanalysis).

Whereas cryptography requires reflexive semantic connections, natural language uses intentional semantics. That is, all forms of natural language expression, or at least the representational ones, use some kind of intentional semantics. It should be noted, and stressed, that the present work very purposefully avoids discussions of how language actually works and does not, and in what ways it is representational or inherently linked to semantics (or not), since these matters are as thorny as they are beyond the scope of study. All that is required for understanding cryptography on these terms is the charitable admission that language does or usually does involve semantics in some important way, linking an "outside" world to particular marks or utterances (in some vaguely realist and commonsense way), and that encryption involves semantics linking mark to mark, with no relevant reference to an "outside" world.

Between natural language and cryptography lie a few boundary-hopping phenomena. Code, or at least some forms of code, are quasi-linguistic (but see chapter six, where I discuss Eco's description of cryptography in terms of code). A modern, quintessential form of quasi-linguistic code is software source code. Source code is human "readable" and yet machine "interpretable." Source code

is thus similar to cryptographic codes of the simple sort, where, for example, an entire word is substituted for another. So long as each code word is cleansed of its (natural) meaning (its reference to an "outside" world), it too can stand in as plaintext notation. In doing so, however, the code word must no longer "mean" what it appears to refer to. If, for example, a simple whole word substitution cipher system defines "cat" to mean "fish" (as in "the fish was purring"), then "fish" must be stripped of its surface semantics, and instead taken as a new atomic part of a substitution cipher, which, *then* means "cat" (the latter semantic connection is only retrospectively perceivable, or post-facto, after the decryption event has occurred).

Whereas code presents some challenges to the analytical precision of my interpretation, the division between natural (written) language and plaintext is perhaps even more puzzling, yet essential (I freely admit that cryptography can play within a linguistic register—in fact, it can make a farce of it, see chapter nine). Indeed, what is the difference between <a> and <a>? None, obviously. And yet, when setting up cryptographic systems, I decree that the prior is a natural written language (e.g., "*a* cat on the mat"), and the latter is plaintext, and thus notational. It might seem that the distinction is without a difference. But, the distinction is without a difference if and only if *no* attention is paid to the meaning and mattering that comes with declaring something plaintext. Indeed, the very act of permitting cryptography in the world is to admit that things are *potentially plaintext*, which means they are *potentially encrypted*.

Even still, if a message is encrypted and then decrypted (from plaintext to ciphertext and then back to plaintext), doesn't this mean the result (plaintext) returns to its status as natural language? Potentially it does, but this is a complicated affair, with a number of factors at play. First, and obviously, many things that are encrypted are never decrypted (think of state secrets or lost Bitcoins). If a message is never decrypted, or if it is only decrypted in certain circumstances, this is, it seems to me, an important distinction to make with respect to the role of cryptography in society. Second, somewhat more subtly, we often ignore the fact (and labour, and consequences) of what it takes to "make" plaintext notation in the first instance. We ignore these efforts because we live in a "chirographic" (writing-focused) world, which also happens to use an alphabetic script, identical to a common form of notation (although perhaps binary is more common today).

The act of *making* plaintext, the first step towards encryption and ciphertext, necessarily involves violence, and identifying this violence is normatively important. As I describe in chapter five, any *thing* can be made into plaintext

with enough effort. That is, this violence of plaintext can be understood as a disregard for the "authentic," or as a lack—in Benjaminian terms, the failure to reproduce the "aura" of the original. We might ask, what does it mean to digitize and replicate a great work of art (even if the reproduction is perfect to the degree of being atomically indistinguishable from the original)? Whether this is an acceptable kind of "violence" to the artwork is a very different and serious thing (which I discuss in terms of allographic and autographic art; see chapter five), and in fact, it is a practical matter for information professionals and those responsible for preservation and access in memory institutions.

This violence, however, is not just the result of mechanical reproduction and remediation. Rather, violence lies at the very heart of the relationship between language and plaintext. A radical version of this claim was made by Derrida, in his *Grammatology*.[30] Derrida believed that violence resulted from differences, gaps, and naming in language; with writing acting as a medium, it interrupted and compromised what would otherwise be a pure and undifferentiated experience of presence. While I am sympathetic to such a view, for my purposes, I only argue that the violence of cryptography results from the difference between natural language and notation. That is, to claim that something is plaintext is to relinquish its hold on the real world, away from the subjects that natural language utterances once held. For example, to utter "cat" is to say something special about the world, since it marks out a domain of meaning (as in denotation: "this is a cat" while pointing at a cat). The plaintext notation <c> <a> <t> may look identical (it has the exact same letterforms), but it no longer marks out the same domain of meaning. In fact, semantically, plaintext points in a different direction from natural language. If "cat" refers to a fuzzy feline sitting in front of the viewer, the plaintext <c> <a> <t> refers to its encrypted form, <r> <q> <b> or even <J3(Q#x_1;A> (recall Alberti's example, where the <a> *means* <g> in the process of encryption). Whereas "cat" has intentional semantics referring to the fuzzy feline, the plaintext <c> <a> <t> has reflexive "semantics" referring to encrypted notation ("reflexive" in the sense that the plaintext points back towards writing, not "out into" the world) (Figure 2.4). To use the word "plaintext" is to admit the *possibility* that an expression is going to be encrypted, which moves the domain of meaning away from human expression, and into the machinic, the ineffable, and the incomprehensible. This shift of meaning and domain is violent and consequential, and is implicitly behind every call to "encrypt everything."

[30] Derrida, *Of Grammatology*.

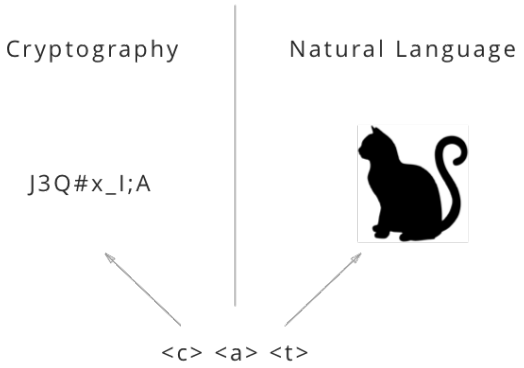


Figure 2.4: Diagram of semantics of cryptography

What the description up to this point does not provide is an analysis of those functionalities *usually* associated with cryptography, such as secrecy (which I have indicated on the diagram with a dashed line to mark its traditional importance, but to indicate its context-specific origins). These functionalities—secrecy and others—are not part of the technical a priori, and thus not directly mapped in figure 2.3. However, the bulk of the present work deals with the ways that these functionalities emerge (and, moreover, this work unearths several functionalities that are not traditionally associated with cryptography). These functions are "positivities" that erupt, in a contingent and historically delimited way, from certain configurations of historical and technical a priori. Secrecy is traditionally the most important of these positivities, but it is far from the only one. Other functions, completely distinct from secrecy, are possible, and even somewhat common in certain historical circumstances. In order to understand how the range of positivities emerge through the conditions of possibility—a vitally important activity for understanding cryptography—I have rhetorically rewritten the conventional terms of art.

Thus, the conditions of possibility of cryptography point to historical accretions of functionality that can be organized into schemata; schemata generated by rewriting traditional terms: plaintext, encryption, and ciphertext. In the typical characterization, plaintext is language, encryption is algorithmic processing, and ciphertext is "secret" code. But in order to expose other positivities—to see the range of what cryptography has been used for—and to understand the historical conditions of possibility, it is necessary to rewrite these terms.

2.3 Rewriting three schemata: Plaintext, encryption, and ciphertext

As a term of art, "plaintext" is an odd word. Ostensibly, plaintext is just text, yet cryptographers have decided that it is an important concept, important enough to invent a new word for it, marking out its special status, which I focus my analysis on. Although this particular distinction has never before been interrogated in the literature on cryptography, the insight is actually a vitally important one. In marking plaintext separate from "mere" text, a whole range of functionalities and cognate phenomena are opened up, such as writing, artificial languages, and proto-computing. Similarly, "encryption" is often understood in a narrow, technological (instrumentalist) sense, but in recognizing that encryption sits *between* plaintext and ciphertext, and is the active agent of change, we encounter an important idea also in need of exploration and rewriting. And finally, despite being the most visible "product" of cryptography, ciphertext has hitherto received scant analytical treatment in the study of cryptography. Typically, ciphertext is either, and only, good or bad (strong or weak), which sits idly by until a decryption process or cryptanalysis attempt turns it back into plaintext. By rewriting the term, I am able to explore the relations between ciphertext elements, and like the analysis of plaintext and ciphertext, expose conditions of possibility, and highlight associated positivities. My approach to exploring these positivities is to rewrite these conventional terms, using this insight to rhetorically guide an archeological exploration.

Chapter three tackles the emergence of a particular kind of plaintext in the fourteenth and fifteenth centuries, during a time that was dominated by representation and resemblances. This era grew out of ancient views of illusion and realism, called mimesis, which underwent a number of significant changes as it emerged out of the Middle Ages. Plaintext writing technologies intersected with shifting influences of mimetic thought and technological development, becoming memory technologies that later became cryptography technologies, as well as the overdetermined concepts of resemblance that constitute a somewhat distinct history of cryptography, here explored in the context of Johannes Trithemius' magical cryptography. Within this context, a counterforce to the mimetic influences developed, in the form of Leon Battista Alberti's notation, which competed with mimetic dogma inherited and adapted from the ancients. With the invention of the movable type printing press, the technical a priori that constitutes cryptography emerged, which, simultaneously, itself became a historically important notational technology. As these mimetic and notational

forces intersected, there emerged a notational epoch, but many authors still remained under the influence of mimetic thinking, even resulting in unusual forms of mimetic "notation." Indeed, at the end of the sixteenth century the concept of plaintext, first articulated by Alberti in the fifteenth century, was still emerging.

Chapter four picks up where chapter three left off, and explores the ways that plaintext grew and flourished through the sixteenth and seventeenth centuries. This chapter focuses on the artificial language planning movement, an attempt to build perfect, universal, and philosophical languages to advance science, peace, and commerce. Early on in this movement, Francis Bacon developed a sophisticated kind of plaintext writing that used binary marks to signify anything by anything. This writing technique was in fact a form of cryptographic apparatus, moving from plaintext to encryption. Bacon believed his writing technique was a tool of cryptanalysis or decipherment of the natural world, as well as a tool of representation—a key part of Bacon's desire to reform language for the new sciences. Others picked up Bacon's language reformation efforts, and a form of artificial language planning that built on cryptographic fundamentals thereafter flourished. In the seventeenth century, nearly any author worthy of Enlightenment aspirations sought the development of an artificial language, which included intellectual giants of the Royal Society, such as John Wilkins. Like Wilkins, most scholars were influenced by their own studies of cryptography, or thought of their artificial language efforts as standing in as a kind of technique of cryptography.

Chapter five moves the archeological investigation of plaintext through the nineteenth, twentieth, and twenty-first centuries. In the nineteenth century, plaintext diminished as a new phonetic form of writing came to dominate, which placed renewed focus on orality, as a quintessentially mimetic form of expression. However, the returned focus on orality was short-lived, as new technologies in the twentieth century encouraged a powerful new kind of notational expression and thinking. Initially, this focus on plaintext was a consequence of the invention of the typewriter (a logical extension of the movable type press), but at the same time, the telegraph and then the computer superseded the typewriter by instantiating networks of plaintext communication. At the close of this chapter, I step back from the historical positivities of plaintext, and offer an investigation of notation itself. The "theory" of notation offered here is an analysis of a priori features that can be read in conjunction with the technical a priori discussed above, since notation subtends all transformations by cryptographic technology.

Chapter six is a transitional chapter that shifts from plaintext to the rhetorical rewriting of encryption. This chapter explores the question of code, which is a quasi-linguistic phenomena that has numerous illuminating connections to the field, technology, and processes of cryptography. I discuss two conceptions of code that make explicit connections to cryptography. The first, by Umberto Eco, is a narrowly proscribed semiotic description of cryptography, focusing on the "correlation" between two sets of symbols in the expressive plane of semiotics. The second, by Friedrich Kittler, ranges much further than Eco's, but in doing so, trades in analytical precision and conceptual tidiness. Kittler's definition of code can be almost entirely understood in terms of cryptography, which makes his analysis uniquely relevant to the present study. I conclude this chapter by analyzing a transitional case study, looking at the cryptographic, electronic poem *Agrippa (A Book of the Dead),* by science fiction author William Gibson (in collaboration with others).

Chapter seven introduces encryption—rewriting the traditional focus on encryption algorithms by investigating the "primal scene" of cryptography. As the primal scene, encryption sits between plaintext and ciphertext, which I argue makes the encryption transformation a mediatic one. This view of media, as "between," originally emerged in Aristotle's psychological work *De Anima*, but the concept was scuttled until the twentieth century when technological forms of mediation made the presence of "media" too obvious to ignore. Indeed, I return to this ancient theme of psychology (from *De Anima*) to reimagine encryption as a form of perception, and archeologically trace the persistent emergence of this theme in the desires for perfect perception and communication, which often entailed the use of cryptographic apparatuses (as with, e.g., telegraphs and Victorian spiritual mediums).

Chapter eight continues the discussion of media, but problematizes the gap between plaintext and ciphertext. Since plaintext is effable and meaningful, and ciphertext is not, I posit the myth of an angel as the functional means necessary to transmit the reflexive "semantics" across the gap between plaintext and ciphertext. Angelic "apparatuses" are a mythical requirement for encryption because humans cannot cross the chasm of meaning necessary for cryptographic media. Such "angels" often take the form of technologies, and we live today in the metonymic influence of their being. I argue that of the available angel myths, Hermes is the traditional angel of encryption, but not the most suitable one. Iris, with her iridescent "sending," is the angel myth most suitable for understanding how encryption works.

Chapter nine focuses on the distinction between decryption and cryptanalysis, using the case study of machine translation. Starting with the artificial language planners (see also chapter four), cryptology has long been associated with machine or assisted translation. In the twentieth century, this idea was explored again, and resulted in the first patents for machine translation (1933). Following the Second World War, Warren Weaver wrote an influential memorandum describing a "cryptographic-translation" idea, which led to modern computerized machine translation. Despite naming his idea "cryptographic," Weaver really had in mind a form of cryptanalysis, which has a unique historical trajectory and is a priori distinct from cryptography. In order to better understand what Weaver might have intended for his idea, I trace the history of cryptanalysis through its Arab invention in the Middle Ages. Arab scholars and bureaucrats developed significant capabilities of cryptanalysis and linguistics, which used sophisticated statistical measures, that would later prove essential for (machine) translation. By the twentieth century, when Weaver was promoting his idea for machine translation, cryptanalysis continued to use probabilistic measures, as described by NSA chief cryptologist William Friedman. I describe the ways that Friedman's work connected to language translation, in terms of grammatical and morphological features and probabilistic measures. I conclude this chapter by describing the analytical basis of cryptanalysis and encryption, showing how encryption is characterized by transcription and the performance of notation, not the probabilistic quasi-linguistic processes of cryptanalysis.

Chapter ten introduces ciphertext, as a form of otherness and order. I discuss Gottfried Wilhelm von Leibniz's exploration of combinatorial forms of order, which he inherited from the long tradition of cryptographers and cryptographically-influenced scholars before him. I then offer a description of the way that order has been understood, focusing on the ways that order is perspectival (and not absolute). In order to show how ciphertext uses order to create perceived disorder, I analyze the artwork of Andrés Ramírez Gavira. Gavira's art engages directly with many themes of cryptography and order, and as a result presents to the viewer a distinct sense of otherness. I contextualize Gavira's art within its history of military technology (through Ivan Sutherland's *Sketchpad* software and the NSA's development of the BLACKER program for online encryption), and use his art to draw aesthetic connections between order, otherness, and ciphertext.

Chapter eleven explores the role of silence, a functional positivity, in ciphertext, by reevaluating an old cryptographic apparatus called the *skytale*. In

nearly every popular history of cryptography, the Spartan *skytale* is discussed as one of the earliest physical tools for cryptography, but in recent years this view has come under attack, lacking philological evidence for the assertion. Rather than critique the philological evidence, I rearticulate the function of the *skytale,* as a device used for creating and maintaining silence, which was a very important social skill in Spartan society. While the *skytale* was often criticized for offering poor secrecy, and therefore suffered the status of being a peripheral cryptographic apparatus (if allowed to be "cryptographic" at all), it did ensure that written words could not be spoken. I then offer an analysis of silence that focuses on the ways that silence is powerful and pregnant, not a simple privation of sound. From this analysis I conclude that the Spartan *skytale*, like any cryptographic apparatus, would have been a powerful and highly effective tool for silence, which should also be considered a peripheral but important historical function and positivity of ciphertext. I conclude by noting that since cryptography can be used to create and ensure silence, it interacts with spoken language. Indeed, cryptography often makes a farce of spoken language, by rendering it silent and ineffable.

Chapter twelve explicitly introduces some of the normative and political themes latent throughout this dissertation. In this epilogue, I critique the contemporary desire to entrench cryptography in every aspect of digital life, which leads to what I call ubiquitous cryptography. This desire for encryption has resulted in a significant homogenization of human expression, parallel to, and in collaboration with, other forces of digital homogenization. Rather than simply oppose the use of cryptography (the Luddite's approach), I conclude by suggesting that new forms of digital politics and resistance might be possible using different kinds of cryptographic tools, using the case study of Bitcoin and blockchain technologies. These technologies might be able to reconfigure the binary of surveillance and secrecy by admitting the existence of potentially politically powerful "open secrets."

In the process of rhetorically rewriting *plaintext*, *encryption*, and *ciphertext*, I describe the processes of cryptography, and the historical a priori. Between the three terms, a natural unity emerges, and a semblance of historical and analytical progression follows. In order to avoid the essentializing impulse of this history that sometimes follows chronological order, I label this semblance of progress a "vector." In the sense I intend, a vector is a trajectory through which technology, information, or media can potentially pass. It has no

necessary position but can link almost any two points together.[31] Thus, this rhetorical rewriting of terms is more than a handy convention to string together the semblance of a narrative. From chapter to chapter and topic to topic, each are analytically framed by vectors pointing to the next, and back again, which at times have been expressed rhetorically in linear fashion, but nonetheless point in many directions.

[31] I adapt the term "vector" from Wark, who in turn adapted it from Virilio. Virilio used the term to describe the (delocalized, permanently moving) trajectories upon which information and military apparatuses can pass, derived from the mathematical sense meaning a line of fixed length and direction but having no fixed position. Wark adapts the term to include media and the media "event," which is how vectors are often discovered. See Wark, "The Weird Global Media Event and the Tactical Intellectual [Version 3.0]"; Virilio, *Speed and Politics*..

Part 1: Plaintext

In this part I rewrite the term "plaintext." Chapter three introduces the unique representational pathways that result from the reconfiguration of writing to plaintext, and describes how plaintext remains indebted to writing technologies, up to the sixteenth century. Chapter four identifies the intersections between the seventeenth and eighteenth centuries' obsession with artificial language planning and cryptography, from Bacon onwards. Chapter five concludes the discussion of plaintext by framing three "discourse networks," and diagnosing how the field of media studies has failed to interrogate the role of cryptography, in contrast to a theory of plaintext as notation.

3
Representation in the fourteenth and fifteenth centuries

In the opening pages of *De componendis cifris*, Leon Battista Alberti (1404 – 1472) introduced his famous polyalphabetic "cipher wheel" while discussing the printing press.[1] In conversation with the papal secretary Leonardo Dati, Alberti noted how the newly invented "system of moveable type… brought us to similar appreciations… [of] strange characters with unusual meanings known only to the writers and receivers, called ciphers."[2] This reference to the movable type press is the first and only in Alberti's entire corpus.[3] But why would Alberti make reference to movable type in a cryptography manual? Kim Williams, the work's modern translator, suggests (on the authority of Anthony Grafton) that Alberti intended the story to function as a dedication, with the hope of having his work printed.[4] However, this reference to movable type is more complicated and more important than Williams or Grafton make it out to be. In fact, this reference is the key to understanding Alberti's cryptographic inventions, and in turn, is the key to understanding the development of modern cryptography. That is, Alberti's reference to the movable type press is a perfunctory admission, or signal, that the invention of the movable type press had a historical and analytical impact on Alberti's thinking when he developed his new form of cryptography. Thus, movable type and cryptography share important historical and analytical connections. These connections reveal fascinating pathways for

[1] *De componendis cifris* was written in 1466 and remained in manuscript form during Alberti's life. A modern English translation by Kim Williams is available in Williams, March, and Wassell, *The Mathematical Works of Leon Battista Alberti*. Reference will be made to this edition, using modern page numbers and section divisions. The modern Latin version has been published in Meister, *Die Geheimschrift Im Dienste Der Päpstlichen Kurie von Ihren Anfängen Bis Zum Ende Des XVI Jahrhunderts*.

[2] Alberti, "De Componendis Cifris," 170. It seems Alberti was aware of Gutenberg's work as well as Arnold Pannartz and Konrad Sweinheim's (who introduced Roman typefaces); see March's commentary, Ibid., 189.

[3] Carpo, *Architecture in the Age of Printing*.

[4] Grafton, *Leon Battista Alberti*, 331. Williams defers to Grafton to make this point, however, Grafton never actually claimed that the reference in *De cifris* was to seek sponsorship for publication. Rather, Grafton claims that Alberti's dedication to G.A. Bussi, in *De statua*, was a request for Bussi, as editorial advisor to Pannartz and Sweinheim, to seek publication of *De statua*. I see no reason, to think that Alberti's mention of a remote "German" in *De cifris* is attempting the same.

the history of representation, cutting across changes in material, linguistic, and architectural forms.[5]

Alberti's *De cifris* was a major turning point in the history of cryptography, which historian David Kahn called the start of a "new species."[6] *De cifris* is a short work, and most of it covers the fundamentals of substitution ciphers and cryptanalysis. In this work, Alberti also described his design for a cipher wheel. The cipher wheel is a mechanism which permits easy realignment between the "index" key and plaintext alphabet. This "index" feature of the cipher wheel was essential to the formation of Alberti's fundamental cryptographic insight—the invention of polyalphabetic encryption.

Polyalphabetic encryption is the process of changing the index letter (at set intervals) during encryption, so that multiple "alphabets" are used for the encryption process. Each time the index letter is changed, new relationships between the source and destination letters are created, which is why the term refers to multiple (poly) "alphabets," even though the group of letters remains the same.[7] It is essential to record the interval at which the index letter is changed, or to use a (known) deterministic method when making the changes, since decryption requires a reversal of the index letter changes. The goal of polyalphabetic encryption is to make a "stronger" form of encryption than is available with a single (mono) alphabet: as each new "alphabet" is introduced in polyalphabetic encryption, the complexity of the resulting ciphertext is increased, thereby making cryptanalysis more difficult.

This cryptographic insight also changed how text was understood to represent the world. After Alberti, letters and words increasingly became plaintext, a form of "technical" representation and latent *matériel* for further cryptographic processing. That is, calling something plaintext, or recognizing that writing is deeply similar to the processes of cryptography, is to align oneself to the logics and affordances of cryptography (and in many cases, subsequent encryption). A similar, parallel, shift occurred with the invention of the movable type press. Together, the movable type press and the cipher wheel introduced reproducible, modular, indexical, and combinatory forms of representation.

In this chapter, I highlight the ways that the material and representational basis of writing were reconfigured by cryptography. In this section, I focus on "plaintext" rather than encryption or ciphertext. I argue that the histories of

[5] An abbreviated version of this chapter appears in DuPont, "The Printing Press and Cryptography: Alberti and the Dawn of a Notational Epoch."
[6] Kahn, *The Codebreakers*.
[7] That is, polyalphabetic encryption expands the combinatorial space of the ciphertext—with each change of the index a new set is added to the total combinatorial space.

plaintext have unique pathways, and that the theory of mimesis, which originally led discussions of representation, eventually proved insufficient to capture the novel logics at play. This representational reconfiguration, from writing to plaintext, was perhaps best and first understood by Alberti. Alberti consciously drew on the ancient theory of mimesis, but he also worked to overturn this traditional model, and was in part responsible for the dawn of a notational epoch, made possible by new code technologies and their conceptual affordances. Nonetheless, although Alberti was essential to the inauguration of the notational epoch, it still very much lay in the future for him, and thus Alberti was a transitional figure, lying between forms of ancient mimesis and a future of notation.

Prior to Alberti, ancient mimetic theory—either Platonic or Aristotelian—was the standard way to think about representation. Leading into the Middle Ages, these ancient theories transformed into a complex web of resemblances. Curiously, in these transformations the resemblance of *convenientia* (convenience) was expressed in the arts of memory. The memory arts were originally developed in late antiquity by Quintilian and other rhetoricians, and picked up resemblances, especially *convenientia,* as Augustine, Aquinas and other medieval authors adapted the theory and practice of memory arts to suit their purposes. In the thirteenth century, Ramon Lull reformed the memory arts again, setting the stage for Alberti's later invention of the cipher wheel. Lull removed imagistic resemblances that had become associated with the memory arts through the Middle Ages. Alberti also developed these theories in his architectural work. These conceptual advances eventually led to the development of the cipher wheel and polyalphabetic encryption.

Shortly after the publication of Alberti's *De Cifris*, the abbot, Johannes Trithemius (1462 – 1516), designed a transmission technology based on cryptographic processes to extend the magical processes of writing. Using the theory and practice built up around the resemblances of *aemulatio*, analogy, and sympathy, Trithemius thought it possible to write across space and time with the assistance of preternatural spirits. Trithemius' method required special (mimetic) performances and careful calculations in order to be successful, which he argued were a part of grammar—not outside of writing, but rather a refinement and extension of writing. This extension of writing was quite unlike Alberti's, however, as Trithemius was not influenced by the invention of the printing press, and in fact, was famously hostile to it. For Alberti, the printing press was a prototype for plaintext, while Trithemius, on the other hand, relied on mimetic concepts rather than typographic, notational ones.

3.1 Epochs of representation

This phrase, "notational epoch," is critical to my historical method and therefore, needs some explanation. As will be described more extensively in chapter five, plaintext *is* "notation" (a scheme of marks or inscriptions with special identity properties of identity, much like discrete marks, or digital symbols), and therefore, as I use the term, a "notational epoch" is an adjustment of the temporal periodization of Friedrich Kittler's term "discourse network," focused on the development of plaintext. Kittler recognized that there can be any number of discourse networks, although he focuses on just two in his *Discourse Networks, 1800/1900*.[8]

To use the specific examples I discuss in chapter five, the discourse network 1800 focused on a new role of pedagogy for educating men. In 1800, the "Mother's Mouth" stood in for all kinds of previous pedagogical experiments, and introduced "universal alphabeticism" through a phonetic method. By 1900, the sounds generated by a mother carefully teaching her son how to explore his "oral cavity" were replaced by standardized and spatialized pure transposition (permutation and combination), exemplified by Nietzsche's blind experiments with his Malling keyboard. The "notational epoch," as I argue it developed, subtends both of these epochs (stretching back to Alberti's *De Cifris* in 1466), and as a historiographical concept, it also recognizes the growing importance of notation as the world moved into Discourse Network 2000.

A discourse network is a configuration of the network of technologies and institutions in an epoch that allows "a given culture to select, store, and process relevant data."[9] Kittler drew on Foucault's notion of schematized epochs of discourse, addressing what Kittler saw as Foucault's lack of attention to technology. The "discourse network," or in the original German, *Aufschreibesysteme* (a neologism invented by Schreber), can be literally translated as "systems of writing down" or "notational systems." As Wellbery notes in his Foreword to Kittler's *Discourse Networks, 1800/1900, Aufschreibesysteme* refers to a level of material deployment prior to questions of meaning, that is, the constraints that select an array of marks from the noisy totality of all possible marks.[10] The totality of all possible marks is not framed in terms of a background absence; rather, plaintext emerges from outside of language.[11]

[8] Kittler, *Discourse Networks 1800/1900*.
[9] Ibid., 369.
[10] Ibid., xii.
[11] See chapter nine for a description of how encryption works outside of language, and chapter ten for a description of how ciphertext is perceived as Other through careful ordering.

A "notational" discourse network is a set of plaintext technologies for the pre-configuration of marks capable of being encrypted, or the set of necessary conditions that encryption acts upon—selecting, transforming, and transmitting *from* the infinite variety of possible forms of expression *to* the potentially massive combinatory space of ciphertext. Therefore, the notational epoch is a long adjustment, through socio-technical "apparatuses," of the representational basis of language, and thus impacts thought and being.

The particular discourse network under consideration here starts back in 1466 with the publication of Alberti's *De cifris* and the growth of a new species of cryptography. The changes wrought by the notational epoch increasingly closed the gap between the human lifeworld and the machinic. And so, since notation enables machine processing in a way that writing simply does not, over time, notation replaced writing in many significant ways.

Despite the ubiquity of encryption today, our notational epoch is still poorly understood. The main challenge to understanding how these technologies work is that we often and erroneously conceptualize a notational epoch in terms of the ancient theory of mimesis. In the last century, dominance of broadcast media technologies until the 1950s—radio, television, and film—meant that most media could be profitably understood in terms of mimesis. But, we now live in the computer era, where digital datasets and algorithms are dominant media. To understand how these "new media" technologies work, we must first understand what the theory of mimesis is, how it changed and adapted through history, and how it was challenged by the kinds of developments sought by early modern cryptographers.

3.2 Mimesis, Resemblance, and Media

Mimesis is the traditional theory of mediation. Since its inception in antiquity, the theory of mimesis was, and arguably still is, about art and aesthetics. That is, mimesis describes the process of making art, and representation more generally, which relies on a duplication of perceived similarity and difference. Eventually, as the theory of mimesis developed, the function of duplication was replaced with repetition and resemblance. Crucially, however, even with these changes, mimesis did not (and does not) adequately describe the way that coded (or "notational") technical media represent their subjects or interact among their parts and wholes.

3.2.1 Ancient theories of mimesis

The origins of mimetic theory are found in the shift from orality to writing. Speech was seen as more natural, and more "present,"[12] than writing, therefore writing was thought to duplicate oral expression. Homer, for example, lived in a primarily oral world. So much so, Milman Parry claimed that virtually every distinctive feature of Homeric poetry was due to its oral mode of composition.[13] The strange, formulaic feel of Homer's plays was a consequence of being "stitched together" from standardized oral expressions (the Greek word for "rhapsodize" means "to stitch song together").[14] Because of this oral mode of composition and communication, Homer's work was the result of an inherent mnemonic structure. Homeric expression includes mnemonic strategies through the processes of rhythm, repetition, phrase addition, redundancy, and many other rhetorical strategies.[15] Without writing, the spoken word is fleeting, so strategies for memory had to be internalized to the mode of expression.

By Plato's day, writing was internalized and used widely. Plato argued that the introduction of writing would cause the loss of memory, since the written word would take its place. The issue of memory, speech, and writing was also taken up in the *Republic*. In this work, Plato attacked all forms of outward expression. Even speech was a duplication of the Forms, Plato argued, and therefore not suitable for the true pursuit of knowledge. More troublesomely, when such duplication was based on false, immoral, and unjust beliefs, it needed to be urgently rejected. The rhapsodes (oral poets) and Homer (first among the poets), were singled out in the *Republic* as promoting this problematic kind of duplication. It is in the context of the introduction of writing that Plato developed his sophisticated theory of representation. In doing so, Plato sought to better understand how speech, writing, and all extant forms of human expression ought to be used; he called this "mimesis."

3.2.1.1 Plato's theory of mimesis

Prior to Plato's *Republic*, the Greek term "mimesis" had a non-philosophical, everyday sense—the act of miming, or a person who mimes. Plato extended and developed this existing sense of mimesis into a full philosophical theory. Central to Plato's theory was a critique focused on how mimetic arts "imitate"

[12] Derrida, *Of Grammatology*.
[13] We know of Homer's work only because after being composed orally, and repeated in memory, it was written down.
[14] Ong, *Orality and Literacy*, 22.
[15] Ong offers an extensive list of the psychodynamics of expression in an oral culture; see ibid., 36 ff.

the deeper reality he posited in his theory of Forms. In this way, Plato's theory was a kind of objectivist one: mimetic art should be judged by its ability to represent the external and objective standards of (ideal) reality. In order to understand the origins of mimesis, I will now turn to the two primary locations for Plato's discussion of it: his *Ion* and *Republic*.[16]

In the *Ion,* Socrates critiques Homer's craft demonstrating that poetry is deficient, or worse, dangerous. Socrates forces the eponymous rhapsode to admit he is only capable of speaking about the poet Homer, which, Socrates argues, is because Ion does not use mastery (*technê*) of a general body of knowledge. Rather, as a poet, he is "possessed" or "inspired" by the Muses. The argument that "inspiration" is the source for poetry is also extended to include other forms of art, such as sculpture, singing, or instrument-playing. In fact, Socrates argues, even Homer himself does not draw upon a body of knowledge—he is also inspired by the Muses.

Socrates argues that inspired art cannot be created when of the "right mind." Just as we sometimes say of artists today, great art is a "divine gift," where over-thinking inhibits the process. God, Socrates claimed, takes the poets' "intellect away from them when he uses them as his servants."[17] This emptying of knowledge has an important consequence for Plato: art does not proceed by way of truth, but is instead a form of madness or irrationality. In what will turn out to be a central difference with Aristotle, Plato aligns *techné* (or "making") with the irrational, inspired source of mimetic art.

Consider another of Socrates' allusions: mimetic representation works like iron rings connected by a magnet. The central magnet puts its power into the first ring, which, in turn, puts its power into other rings, and so on, until the magnetism is finally used up.[18] Accordingly, Homer is the first, most divine ring, having received his poetic gift directly from the Muses; Ion is a more distant, lesser ring, who does not possess the same divination as Homer. Homer's work is therefore representative of the divine, but Ion's recitations are worse: he is a mere representative of a representative (doubly imitative). Each more distant ring from the original inspiration is a further derivation (and depletion) of whatever reality and truth the original might have possessed.

The theory of aesthetics that was advanced in the *Ion* focused on the ways that art can be derivative and false. In this early work, however, Plato does not use the term "mimesis." By the time Plato wrote the *Republic*, a fully mature work

[16] English translations from Plato, *Complete Works*.
[17] *Ion*, 532c.
[18] *Ion*, 533d.

of politics and metaphysics, he had developed the robust theory of Forms, and therefore could incorporate and further develop the aesthetic theories he explored in the *Ion*. In doing so, Plato called on the term "mimesis" to buttress his normative theory of art.

In Book III of the *Republic*, Socrates and Adeimantus discuss the role of mimesis in their proposed ideal state. Socrates formally introduces mimesis in Book III, it being a kind of performance, or "story-telling."[19] Certain public discussions must be restricted, they argue, because they are liable to be imitated by the youth and therefore potentially bring about negative effects. Indeed, Socrates argues that the "style" or "how it should be said" of some discussions must be restricted, as well as the content.[20] Alluding to his theory of aesthetics in the *Ion*, Socrates argues that an imitative poet must "hide himself."[21] Once again, Socrates is concerned that mimesis functions without mastery or skill, and is used by those who fail to "achieve distinction."[22] Therefore, poetry and all imitative arts should be restricted in both content and form in the ideal state.

In the *Republic*, Plato extends the aesthetic approach of the *Ion* to morality and politics. According to Plato, slavish or shameful actions are caused by the creation of a derivative, false reality—an imitation of the real world.[23] This problematic imitation of the real world also extends into personal belief and behaviour and social relationships, which corrupts otherwise good people. This cause and effect of mimesis, famously, is like a drug: it is powerful and useful when administered correctly, but dangerous when used improperly.

In Book X, Plato continues his discussion of how the origins of mimesis are irrational and illusory, that its drug-like effect leads to troublesome personal and social behaviour. In a discussion with Plato's brother, Glaucon, Socrates extends his earlier prohibition of poetry to all imitative arts. For this argument, Plato claims that there are three levels of reality,[24] exemplified by the maker of a couch: first, there is the idea of a couch, made by god—the "natural maker"—which is necessarily singular and most real; second, there are material couches made by craftsmen who strive to be like god, imitating the original Form, but who do not "truly make [*poiesis*] the things themselves;"[25] and third, there are the imitative artworks, made by painters and as such do not imitate the original

[19] *Republic*, 394c.
[20] *Republic*, 392c.
[21] *Republic*, 393d.
[22] *Republic*, 394d.
[23] *Republic*, 395c.
[24] *Republic*, 597ff.
[25] *Republic*, 596e.

but simply imitate the (imitated) material works of craftsmen. To show how false and illusory the craftsmen and the painters are, Socrates imagines a "clever and wonderful fellow" who walks around with a mirror and claims to be "making" all the things of the world as he points it towards objects.[26] This fellow with the mirror, obviously, is only fabricating the "appearance" of things. This metaphor extends to non-visual forms of mimesis, too. In fact, Plato often aligns the formal qualities of visual arts (colours and shapes) with the mimetic qualities of poetry.

And so, in Book X, we see a serious ontological and epistemological challenge to mimesis. Like the famous "allegory of the cave," discussed earlier in the *Republic*, a complete shift in ontological thinking has occurred: truth is no longer to be found in the material things of the world (neither the material couch nor the painting of it). Instead, truth resides in the intellect alone. Plato believed that the world we see and experience, like mimetic art, is a mere imitation of a deeper, non-mimetic reality.

3.2.1.2 Aristotle's theory of mimesis

Aristotle's views on mimesis are found, for the most part, in his *Poetics* (the same work that introduces, but dismisses, the concept of "media"). In this work, Aristotle describes several issues of aesthetics. He provides detailed criteria for differentiating between forms of art; discusses the source of mimetic arts, as rational and structured; and, details how mimetic arts aid in education, ethics, and pleasure. In general, Aristotle's view of mimesis is in reaction to Plato's critical appraisal, made possible by, specifically, Aristotle's interrogation of the concept of *muthos*. Before Plato, *muthos* simply meant "content," but Plato adapted it to mean distorting "myth," which he looked upon unfavourably. Aristotle further developed the term, and made it an important aspect of his theory of mimesis.

The bulk of the *Poetics* is devoted to differentiating between forms of mimetic art—differentiating between poetry, tragedy, and epic, while also contrasting visual arts (such as painting and sculpture). Poetry, for example, can be analyzed by "differences in character" within narratives.[27] Tragedy is distinct from poetry, being an imitation of a "serious" action that is "complete in itself" (in the sense of being rational and structured).[28] Tragedy can also be pleasurable despite its "serious" topic—even, in fact, when the topic is "painful to see."[29] While the

[26] *Republic*, 596d.
[27] *Poetics*, 1448b25.
[28] *Poetics*, 1449b20.
[29] *Poetics*, 1448b10.

pleasure from tragedy is unique and offers different opportunities for education, it is, however, just a species of a more general pleasure from mimetic art, like the pleasure of poetry or epic.

A central concern for Aristotle is *muthos,* which he reimagined as "plot-structure."[30] Whereas *muthos* was almost exclusively pejorative for Plato, Aristotle reimagined it in a positive light. According to Aristotle, "plot-structure" is formally the abstract shape of a narrative plot, but also the totality of the represented action, with all its causal connections and development.[31] Aristotle argued that a correct *muthos* must not simply string together mimetic events into a narrative, rather, the structure must be "complete in itself, as a whole of some magnitude."[32] This "whole" must have a beginning, middle and end that are "naturally" connected. It is the *muthos* structure that creates a feeling of completion, direction, and justifiable connection within a plot (versus a plot that lacks compelling direction, zigging and zagging without reason). According to Aristotle, good plot-structure is created by the mimetic connection to reason, not inspiration or madness, as Plato had previously argued.

Aristotle argued that there are two natural, human causes of poetry, both grounded in mimesis. First, from childhood we are naturally imitative, and second, we take pleasure in works of imitation.[33] Because these are such powerful psychological forces, Aristotle figured that mimetic arts could be beneficial in education, and useful to help align moral issues. In fact, the educational value of mimetic art is closely associated with its ability to provide pleasure to its audience. Learning is itself "the greatest of pleasures,"[34] Aristotle argued, yet mimetic art can also "gather the meaning of things," helping direct one's gaze from particulars to universals.[35] Some mimetic arts are fictional or truly novel, in which case there is very little realism or verisimilitude, and the viewer does not have an existing referent for the mimetic subject. Despite not possessing a clear concept of the referent, these arts can also be educational and pleasurable. In such cases, when mimesis is purely fictional and novel, Aristotle claimed, the educational and pleasurable value does not simply lie in the formal

[30] Plot-structure is about narrative plot as we might typically see in a story or play, but the concept also extends to less narrative arts. As Aristotle describes it, a painting or a sculpture can have a "plot-structure."
[31] Halliwell, *Aristotle's Poetics*.
[32] Ibid., 5.
[33] *Poetics*, 1448b5.
[34] *Poetics*, 1448b10.
[35] *Poetics*, 1448b15.

qualities of the mimetic art—"the execution or colouring or some similar cause"—but rather, education and pleasure are caused by the *muthos* of the representation itself,[36] that is, its rational structure.

Aristotle argued that aesthetics should be conformable, if not subject to, moral and political principles, and should still be consistent with reality (especially reality perceived through universals). For example, a horse drawn correctly but with poor talent is not as good as a horse drawn with a technical error (e.g., legs facing the wrong way) but nonetheless does not fail "in the essentials of the poetic art."[37] Similarly, it is better to portray good men ("as they ought to be"), instead of bad ones, but precedence should be given to how artistically the activity is conducted. In summary, the Aristotelian theory of mimesis still articulated representation in terms of normativity and illusory duplication.

While sophisticated and various in their approaches—Plato opposing mimesis in favour of his own ontological approach, Aristotle seeing considerable value in mimetic arts—ancient views of representation were still fundamentally configured around illusions and realisms. As the ancients understood it, making art and, more generally, human expression, relied on the duplication of perceived similarity and difference. The question of representation, as the theory of mimesis developed, and especially as newer "media" technologies came into use, stood in for the ways that duplication was eventually replaced with notions of repetition and resemblance, and thus as it produced new associations, uses, and historical pathways.

3.2.2 The age of resemblances

As the ancient theories of mimesis were taken up in new contexts, and for new purposes, illusion and duplication became forms of repetition which pictured the "universe… folded in upon itself."[38] From the fall of Rome until the Renaissance, the Greek term and the original philosophical concept of mimesis fades, only to be replaced with an extremely rich semantic web of repetition and resemblances. The periodization of these developments also becomes more complex, since by the end of the sixteenth century, all exist and interrelate at once. Each new sense of representation rewrites Plato's and Aristotle's mimetic theories, and from this process emerges—haltingly and somewhat opaquely—a new age of resemblances.

[36] *Poetics*, 1448b20.
[37] *Poetics*, 1460b20.
[38] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, 19.

At the same time, many code technologies emerge. It is within this context of mimesis and the shift to resemblances in which we can locate Alberti's cipher wheel and the invention of polyalphabetic encryption. Other cryptographers, such as Trithemius, are also situated within this changing historical landscape. Ultimately, the practice of cryptography throws up new technical challenges, and the theory of mimesis was poorly suited to explain. Guided by these technical challenges, cryptographers offered early critiques—and accommodations—of the extant theories of representation, and in doing so advanced new forms of praxis. Many scholars would later attempt to cleanse these mimetic holdovers, pining for modernity—scholars such as Descartes, who in the early seventeenth century sought to eliminate the very category of resemblance from true epistemology.

To understand the representational landscape up to the sixteenth century, I follow Foucault's schematization of resemblance in *Order of Things*, itself an archeology of representation and order. Foucault identifies ten such notions in the late medieval and Renaissance web of resemblances, gathered from the jurist, Pierre Grégoire's *Syntaxeon artis mirabilis.* Of these ten, Foucault states that four are essential to understanding resemblances at the end of the sixteenth century: *convenientia, aemulatio,* analogy, and sympathy.

3.2.2.1 Convenientia in memory technologies

The theory of *convenientia* (convenience) emerges within the history of memory arts. According to Foucault, *convenientia* denotes adjacency of places, where things are close to one another.[39] In antiquity, techniques for the art of memory focused on mental "locations," but over time mimetic images were added to this method. As resemblances were reconfigured in the discourses, *convenientia* came to play a larger role in people's understanding of memory techniques. New code technologies were also developed, which transformed memory techniques into memory technologies. One of the principle reconfigurations of memory technologies was, of course, the development of the book itself, but, rather surprisingly, up until the sixteenth century, old fashioned memory techniques did not disappear, as one might have expected when books became more prevalent. Instead, the memory arts adapted throughout this period, first adding mimetic imagery, and then shedding some of the mimetic imagery that was acquired during the Middle Ages. Drawing on the tradition of memory arts and *convenientia,* Ramon Lull also produced a technique and technology suitable for combining and analyzing aspects of the natural and supernatural

[39] Ibid., 21.

worlds. This technique of combining and analyzing would ultimately influence Alberti's innovations in cryptography.

Of the three most famous mnemotechnical works in antiquity, Quintilian provides the clearest picture of the method (but his work, with its clear exposition, was lost through the Middle Ages). As Quintilian describes it, to fix items firmly in the memory, one must place the items to be remembered within a mental architectural scene, typically, mentally placed within one of the houses along a well-known street. In later incarnations of the technique, items were mentally fixed within a room that contained special nooks for mental placement (these places were called "*loci*"). To recall the items from memory, in the mind's eye, one only has to move from one place to the next (from house to house or nook to nook). The basic method could be further refined (and over the years there were many adaptations), for example: each fifth item could be given a distinguishing mark (to help keep track of the location in the sequence); the memory places could be made very distinct and not too crowded; the technique could use "words" instead of "things;" and (as was particularly common in the Middle Ages) adding arousing images would help mentally focus items within the *loci*.

Unlike most ideas from antiquity, knowledge of the art of memory did not depend on transmission through the Christian Fathers or the Arabic translators. The art of memory was known, it seems, directly through the lively rhetorical tradition (specifically through the *Ad Herennium*).[40] However, when Rome fell, the rhetorical tradition was no longer supported by Rome's institutions, and so, the rhetorical tradition changed, and the art of memory followed. Throughout the Middle Ages, the rhetorical tradition was sustained by religious orders, and so, the art of memory came to be used exclusively for remembering pious things, as a mechanism to assist natural devotion. And with these new religious associations, the art of memory became an ethical practice, linked again to normative issues, just like mimesis during antiquity.

In the late Middle Ages, the most significant and far-reaching alteration of the method came when Thomas Aquinas (1225 – 1274) replaced the architectural scenes, previously used for memory *loci,* with a method based on "corporeal [and convenient] similitudes."[41] These are strange changes: while the original technique had already been adapted for use with religious devotion, Aquinas' method introduced corporeal or even profane imagery. The use of corporeal similitudes was necessary, Aquinas reasoned, because "it is natural for man to

[40] Yates, *The Art of Memory*.
[41] Ibid., 76.

reach the *intelligibia* through the *sensibilia* because all our knowledge has its beginning in sense."[42] And what to provoke the *sensibilia* than wild and wonderful images?[43] Once Aquinas planted the seed, the technique flourished.

Aquinas' method would enter into the Renaissance's own complex web of resemblances. In his *Summa*, Aquinas provided no examples of the kinds of images to be used, but others would take up his suggestion. Organized in convenient order, the images for the corporeal similitudes would be drawn from all aspects of life (see e.g., J.H. von Romberch's sixteenth century adaptation of Aquinas' method; Figure 3.1). As hermetic imagery became popular, it too joined Aquinas' method for memory arts, using shocking images of beasts and devils. Yet, at the same time, a revival of the ancient architectural (non-pictorial) method was also occurring.

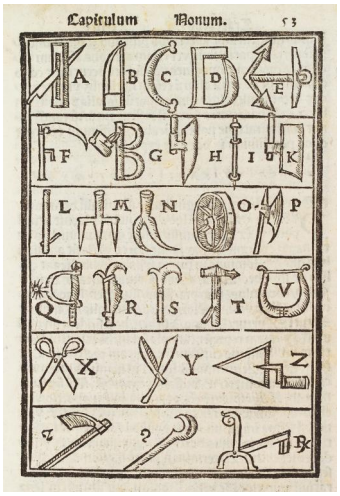


Figure 3.1: "Visual alphabet" from J.H. von Romberch's *Congestorium Artificiose Memorie* (1520).[44]

One would expect the influence of memory arts to wane with the introduction (and flourishing) of the printed book in the fifteenth century, which ought to obviate the need for memory techniques even more than the introduction of the written word. However, leading up to the Renaissance, more careful study of the ancient techniques of memory helped to expose the medieval "perversion" of adding similitudes (this reformation was aided by the re-introduction of Quintilian's work, and a clear exposition of the art).

---

[42] *Summa Theologica*, I, I, question I, article 18.

[43] Aquinas writes: "[H]e should assume some convenient similitudes of the things which he wishes to remember; these should not be too familiar, because we wonder more at unfamiliar things and the soul is more strongly and vehemently held by them." *Summa Theologica*, II, II, question 49, article I.

[44] Romberch, *Congestorium Artificiose Memorie*, 53.

At the dawn of the era of printed books, in the fifteenth century, the memory arts returned to an architectural model, based on *convenientia* of items in a "memory theatre." This memory theatre method was inspired by the body of writing known as the *Corpus Hermeticum*, rediscovered and translated into Latin by Marsilio Ficino (1433 – 1499) (the *Corpus Hermeticum* was believed to be of ancient Egyptian providence, written by one Hermes, or Mercurius Trismegistus). Inspired by Ficino's translation and his considerable influence, Giulio Camillo (c. 1480 – 1544) constructed an actual memory theatre, making extensive use of the conceptual parallels between the microcosm and macrocosm in hermetic and Neoplatonic thinking.[45] The theatre was an adaptation of the practical *loci* method of memory, inherited from antiquity, and Camillo designed his memory theatre to literally reflect humankind's place within the universe. Camillo designed the *loci* in the theatre as a microcosm of the universe—arranged, numbered, and named in accordance with a true reflected reality. Impressive feats of memory were possible, it was believed, because the theatre let its users tap into a divine memory.

From antiquity and the Renaissance, *convenientia* grew in importance, as a critical component of the web of resemblances. As an ancient technique of rhetoric, it was employed as an art of memory that functioned quite distinctly from ancient mimesis. By the Middle Ages, however, these "*loci*" resemblances lost some of their purely "convenient" characteristics of adjacency, and picked up more imagistic, mimetic qualities. By the Renaissance, mimetic resemblances had accreted new Neoplatonic properties that used images to a greater extent, becoming a method that dug deep into reality, and posited the world as a reflection of an emanative first principle. Yet, as some theories of *convenientia* weaved into mimetic territory, others—such as Ramon Lull's theories—veered in the other direction, removing the use of images, and purifying the art from mimesis.

3.2.2.1.1 Ramon Lull, convenientia*, and the path to Alberti*

The Catalan thinker, Ramon Lull (1232 – 1315), was a contemporary of Aquinas, but blazed a new path for *convenientia* and the memory arts—a path that would ultimately lead to the invention of Alberti's cipher wheel. As we saw above, Aquinas was an important figure in the history of *convenientia* for the memory arts, but for him resemblances included corporeal similitudes, which later became Renaissance memory theatres.

[45] Yates, *The Art of Memory*.

Like Aquinas, Lull worked within a Christian context, but Lull does not seem to have been influenced by Aquinas' work (Lull was apparently out of touch with contemporary Parisian scholastic trends).[46] Instead, Lull's theories for his "Art" (*Ars*) draw from Augustinian Platonism, with elements of popular Neoplatonism. (And due to his interaction with Arabic philosophers, Lull might have also been influenced by Arab astronomy, and the myriad devices used for calculating the heavens.) Whatever the origins, Lull's Art can be compared and contrasted to the existing model of *convenientia,* from Aquinas to Camillo: it resulted in a re-configuration of the web of resemblances, a rejection of mimetic images in the arts of memory, and a place of importance for normativity in memory practices.[47]

Lull's art differed in important ways from the mainline version of memory arts. First, Lull's Art did not originate from the rhetorical tradition. For Lull, the memory arts served a Christian god, as one part of three methods unified under one Godhead in the Christian Trinity: *intellectus*, an art of knowing and finding Truth; *voluntus*, an art of training the will towards loving Truth; and *memoria*, an art of memory for remembering Truth. This is in sharp contrast to the rhetorical tradition, which, by the Renaissance, had sought to duplicate the world and gain access to it through a series of similitudes and images. Second, drawing on Plato's critique of mimesis, Lull opposed the use of mimetic representations. This was distinct from the medieval use of images, which were used for exciting the memory, an aspect of the method encouraged by Aquinas. In place of these mimetic images, Lull used clear and precise notation to help hold items in the memory. Each item was combined according to particular rules, which amounted to a generalized method for investigating reality. Third, Lull adds movement to an otherwise static tradition. Before Lull, memory items were held in place as static *loci*. Lull introduced rotating wheels, so that memory could dynamically contribute to knowledge.

In Lull's *Ars Brevis,* the first "figure" arranges the divine "dignities" (first causes) into two circles, with each segment designated by a single principle, aligned against another (see Figure 3.2).[48] The outer ring of nine letters (B, C, D, E, F, G, H, I, K) aligns against the inner ring of dignities, arranged in *convenientia* (in the first figure, which is denoted by "A," the dignities are Goodness, Greatness, Eternity, Power, Wisdom, Will, Virtue, Truth, and

[46] Llull, *Doctor Illuminatus*, 76.
[47] A translation of some of Lull's work, including the *Ars Brevis*, is available in Llull, *Doctor Illuminatus*.
[48] There are several figures to Lull's art, and they developed during his prolific career. In the *Ars Brevis* the first, second, and fourth figures are circular, while others use a tabular format.

Glory). As the reader compares the inner and outer circles, new propositions are created, such as "goodness is great" and "greatness is good."[49] And then, in figure four of the *Ars Brevis,* Lull adds another ring, removes the names of the dignities, and makes each ringed plane rotatable (see Figure 3.3). With this paper apparatus—also known as a volvelle—the reader can explore new associations and predicates, as the planes rotate and realign dignities. The tool is effective "because each letter can have many meanings," which, Lull notes, helps "the intellect become… more general," akin to the way that the mind moves from the particular to the universal in Aristotelian epistemology. This mental movement upwards is made concrete in Lull's third figure: the intellect climbs a graphic "ladder" as combinations are understood.[50] Each item of the method, along with "the alphabet" and their signifieds, must be "learned by heart."[51] Therefore, each letter also works like the *loci* of the memory arts, holding in the mind a particular notion for consideration and mental investigation. Lull notes that each turn of the wheel, which is in a Trinitarian design, activates the Will (*voluntus)*, which prompts the Intellect (*intellectus)* to consider the resulting combination, and fixes the *loci* of the proposition in the Memory (*memoria)*.

[49] Llull, *Doctor Illuminatus*, 301.
[50] Ibid., 303.
[51] Ibid., 298.

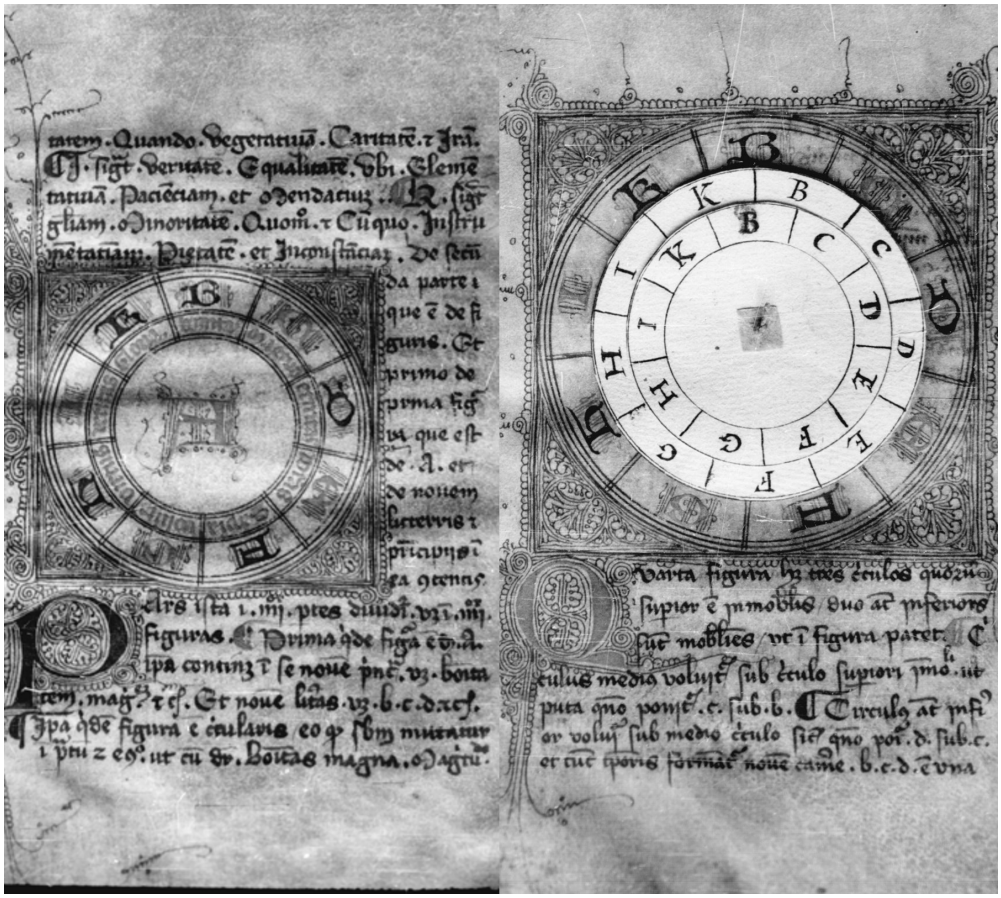


Figure 3.2 (left): First figure, denoted by A, and Figure 3.3 (right): Fourth figure, from Lull's *Ars Brevis* (1308/1584).[52]

There is an interesting coda to this narrative that bears mention: nearly three hundred years after Alberti, and some four hundred after Lull, Gottfried Wilhelm Leibniz (1646 – 1716) wrote his *Dissertatio de art combinatoria,* developing Lull's and Alberti's early investigations into a systematic programme of the study of order, which is today the mathematical study of combinatorics.[53] In this work, Leibniz divides the study of "relations" into two categories: one of "union" and one of "*convenientia.*"[54] However, Leibniz rejected the utility of studying *convenientia*, accusing his Scholastic predecessors of mistakenly believing that "number arises from the division of the continuum."[55] Rather, Leibniz argued that it is "analysis" and "arithmetic" (not *convenientia*) that are

[52] Llull, Ars Brevis. Biblioteca El Escorial, Madrid Ms. f.IV.12. The outer paper rings on the manuscript are a reconstruction.
[53] See chapter nine for a further discussion of Leibniz's systematic study of order.
[54] Leibniz, "Dissertation on the Art of Combinations," 76.
[55] Ibid.

comprised of number.[56] That is, the focus of Leibniz's method is the division of "union" into parts and wholes, with attention to their variations and relationships. By turning away from *convenientia*, Leibniz is finally freed to systematically investigate the relationships of discrete finite objects without needing to account for hidden relations between things. And so, resemblance is finally purified.[57]

Prior to Leibniz's distinction, however, when representation aligned to mimetic theory, there was slow progress towards new and functional code systems. Ultimately, this is what happened to Trithemius' cryptography, who introduced many strange and wonderful resemblances to the study and practice of cryptography.

3.2.2.2 Aemulatio, Analogy, and Sympathy in Trithemius' Magical Cryptography

The remaining three *resemblances—aemulatio,* analogy, and sympathy—are all alike functionally, and related to *convenientia,* but also associated with communication media rather than memory technologies, as discussed above.

Aemulatio is, according to Foucault, "a sort of convenience [that is, *convenientia*] that has been freed from the law of place and is able to function, without motion, from a distance."[58] Since *aemulatio* is free to function at a distance, it is the "means whereby things scattered through the universe can answer one another."[59] Like the ancient theory of mimesis, *aemulatio* is a duplication within a mirror, but "abolishes the distance proper to it."[60] And since the ability to abolish distance is a key feature of media technologies, *aemulatio* can therefore be considered a key form of representation for media and media technologies.

Analogy is the old theory of mimesis, but given powers of universal application, drawing together the entire universe as a superimposition of *convenientia* and *aemulatio*. Analogy makes comparisons possible, just like the mirroring involved in *aemulatio*. Analogy, however, mirrors and inverts: both *aemulatio* and analogy draw the universe together, but only analogy places humankind at the privileged point, capable of making comparisons. For example, consider the comparison: "the plant is an upright animal," which is

[56] Ibid.
[57] In chapter eight I describe how Leibniz uses this distinction to develop calculating and encrypting devices.
[58] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, 21.
[59] Ibid.
[60] Ibid., 21–22.

inverted as, "the root [is] in the lower part of the plant and the stem [is] in the upper part, for the venous network in animals also begins in the lower part of the belly, and the principal vein rises up to the heart and head."[61] Such strange comparisons, between plants and animals, are possible only because human beings are the "fulcrum" upon which these relations turn.[62]

Sympathy is a "principle of mobility" because it attracts like things together: roots toward water, sunflowers to the sun.[63] Foucault argues that sympathy is an instance of the "Same," so strong and so insistent that it displaces likeness (and thus illusory senses of mimesis); it is a power of assimilation that renders things identical.[64] Natural magic made good use of sympathies. For example, a tooth and a pinecone are magically sympathetic because they share certain visible resemblances, and therefore share interior qualities that are capable of standing in for one another. Or consider, for example, Foucault's descriptions of similar looking things, which are typical of sympathetic thinking: "aconite will cure our eye disease, or that ground walnut mixed with spirits of wine will ease a headache."[65] Sympathy is ultimately hidden in some way (it is an interior relation), but "there must of course be some mark that will make us aware of these things," so that they can be used.[66] Recognizing these marks of sympathy is an essential part of occult science.

The hidden mark of sympathy is a "signature," which provides evidence of how resemblances are associated, and thus, must be identified and deciphered. The signature "is the science by which everything that is hidden is found."[67] In fact, "there are no resemblances without signatures," Foucault writes, because knowledge of resemblances is based on identifying and deciphering signatures.[68] For example, the title of book nine of Paracelsus' treatise *De natura rerum* is "De signature rerum naturalium," an explicit reference to the signature of natural things.[69] In this work, Paracelsus argues that Nature does not "release anything in which it has not marked," as though the interior is visible from the exterior.[70] Therefore, signatures are vitally important for the web of

[61] Ibid., 24.
[62] Ibid., 25.
[63] Ibid., 26.
[64] Ibid.
[65] Ibid., 29.
[66] Ibid.
[67] Agamben, *The Signature of All Things*, 33.
[68] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, 29.
[69] Agamben, *The Signature of All Things*, 33.
[70] Ibid.

resemblances, offering marks that allow identification, comparison, and analysis.

Put together, these three resemblances draw the mind away from changing (and superficial) particulars and towards universals. For miraculous phenomena that plumb the depth of reality—which all people of the era believed existed—the senses alone are insufficient for attaining knowledge. Now that we understand how the three remaining resemblances worked, we can explore the magical cryptographic processes and technologies Johannes Trithemius developed.

The scholar and cryptographer, Johannes Trithemius (1462 – 1516), believed that using the correct notation, or "character," was a vitally important step to identify, and indeed attract, the appropriate spirit for deeper knowledge. The wrong identification, of spirit or mark, prohibits the ability to know the thing. Indeed, knowledge and technical communication hinge on the web of resemblances, which (Trithemius believed) enable thought to work at a distance. For Trithemius, the cryptographic processes are able to fold things together, in order to bring the distant close, which is how sense, as a kind of interpretation, is made in the world.

Trithemius wrote two cryptographic works: the infamous *Steganographia*, dogged by accusations of demonology, and a sanitized version written subsequently, the *Polygraphia*.[71] The *Polygraphia* included designs for a transposition cipher, as well as a cipher wheel (in book five), similar to Alberti's invention from several decades prior (see Figure 3.4). Like Alberti's invention, the cipher wheel of the *Polygraphia* uses a true polyalphabetic cipher (whereas the *Steganographia* includes designs only for a partial polyalphabetic cipher). Despite being less sophisticated, the *Steganographia* was more infamous—known widely while it was still being written, and circulated as a manuscript before its posthumous publication in 1606 (then bundled with a "key" or *Clavis,* written by Trithemius himself).

[71] The only extensive description of Trithemius' *Steganographia* is only available in German: see Ernst, *Schwarzweisse Magie. Der Schlussel Zum Dritten Buch Der Steganographia Des Trithemius.*

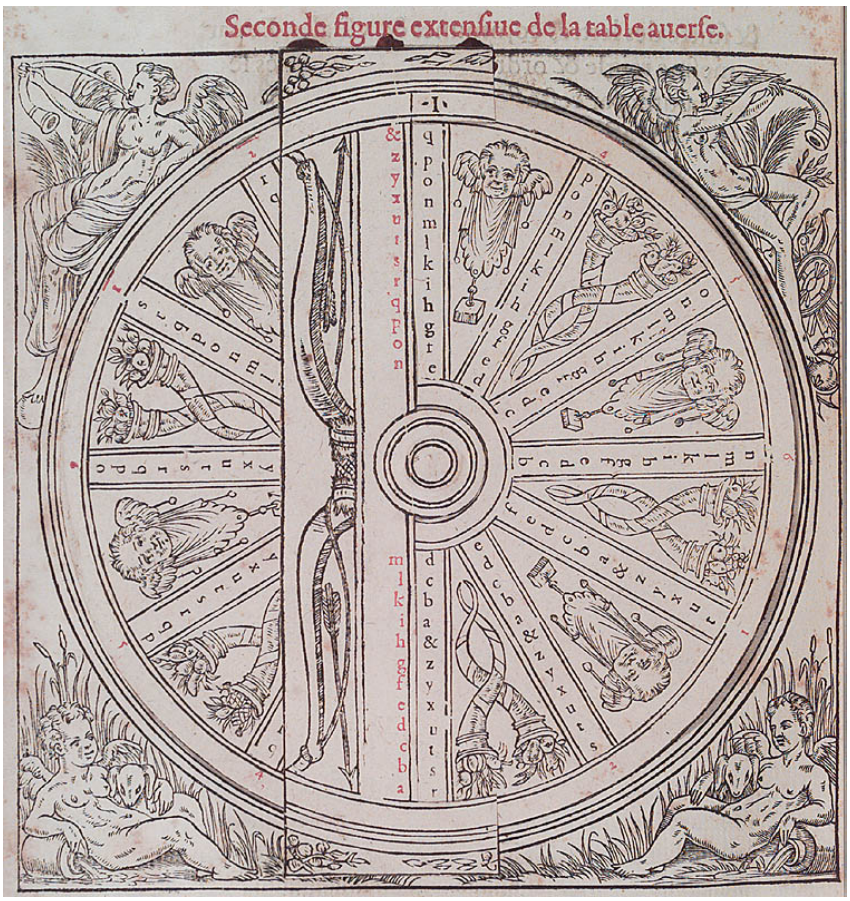


Figure 3.4: Cipher wheel from book five, figure two, of Trithemius' *Polygraphia* (1561).[72]

The third book of the *Steganographia* was never finished, but the manuscript was widely sought, as it was thought to include designs for communicating through black magic and demonology.[73] Early on, colleagues of Arnoldus Bostius accused Trithemius of demonology,[74] causing Trithemius to scuttle the project and instead take up writing the *Polygraphia* (1518), a version of the *Steganographia* free from discussion of intermediating spirits.[75] Later (c. 1503 –

[72] Tritheme, *Polygraphie: Universelle Escriture Cabalistique de M.I. Tritheme Abbé*.
[73] John Dee had managed to copy half of the manuscript and unsuccessfully offered "a Thouwsand Crownes" for the rest; Shumaker, *Renaissance Curiosa*, 97.
[74] In 1499, Trithemius wrote to his friend Bostius, but by the time the letter had arrived Bostius had died. Bostius' colleagues read the letter and saw Trithemius' boasts of what the *Steganographia* was capable of, and accused him of being either a liar or a demonologist. See Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia," 293.
[75] Ernst offers a careful description of the complicated manuscript and publication history. The *Steganographia* was actually composed of three parts, with a separate manuscript as an early version written between December, 1498 and March, 1499. The *Clavis* attached to the 1606 printed version bears resemblance to an earlier *Clavis specialis*, written after March, 1499 and

04), the French mathematician Carolus Bovillus visited Trithemius and read some of the incomplete *Steganographia*,[76] and in a 1509 letter accused Trithemius of demonology. When the letter was published a year later, Trithemius' reputation for working with dangerous spirits was firmly established, and haunted him until his death, six years later.

Despite its associations with demonology, many future cryptographers tried to harness the lessons of the *Steganographia*. "Gustavus Selenus" (pseudonym of Duke of Brunswick-Lüneburg, 1579 – 1666) wrote his *Cryptomenytices* (1624) with liberal quotations from three versions of the *Steganographia,* even going so far as to print the entirety of book three, hoping that some future cryptographer might be able to supply a solution.[77] Similarly, Gaspar Schott (1608 – 1666) devoted two sections of his *Schola steganographica* (1655) to the interpretation of Trithemius' challenging work. Other works, inspired instead by the *Polygraphia*, and therefore free of demonological aspects, soon appeared. Perhaps the most famous was Giovanni Baptista della Porta's *De furtivis literarum notis, vulgo de zipheris, libri quinque* (1602).

Trithemius described his introduction to cryptography as the result of a book buying trip to stock the famous Sponheim library.[78] On this trip, Trithemius encountered an old work on Tyronian notes in a Benedictine library, which he acquired in exchange for a new manuscript of St. Anselm's. Although today we would recognize Tyronian notes as a form of shorthand writing used by Cicero's secretary, at this time they were considered a form of cryptography. Of course, Trithemius eventually became aware of other sources for cryptology, and included a history of the subject in the *Steganographia* and *Polygraphia*, which also included the Caesar substitution cipher, and a discussion of the origins of language.[79]

The first two books of the *Steganographia* offer a fairly straightforward discussion of coded language, couched in examples of spirit conjurations. Shumaker offers the following example and interpretation (taken from the 1606 *Clavis*):

---

discontinued in April, 1500. Furthermore, whereas the *Clavis specialis* contained plain-language descriptions of the cryptographic processes, when included in the *Steganographia* these parts were reworked into a kind of "arcane" language. See Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia," 319.

[76] Ernst gives the date as 1503 – 04, but notes that it is unclear. See Ibid., 320.

[77] Shumaker, *Renaissance Curiosa*, 100; Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia," 295. See also Strasser, "The Noblest Cryptologist."

[78] Grafton, *Worlds Made by Words*, 62.

[79] Shumaker, *Renaissance Curiosa*, 94, 112.

Pamersiel Anoyr Madrisel Ebrasothean Abrulges Itrasbiel

Nadres Ormenu Itules Rablon Hamorphiel

Shumaker decrypts the example as such: if we ignore the first and last words (known as "nulls," which are inserted to help obfuscate the message), we can decode the message by reading alternate letters (here in **bold** type). The message is: "*Nym die ersten Bugstaben de omni uerbo*" ("Take the first letters of every word").[80] In the remainder of the first two books, Trithemius offers other examples of coded language, some with more complicated encodings of the same basic pattern (including the use of a single alphabet substitution cipher). As in the later *Polygraphia*, the spirit names invoked in the first two books of the *Steganographia* were not "functional," rather they provide a "key" as a kind of password for decoding the messages. The third book of the *Steganographia*, not included in the 1606 printing and not part of the *Clavis,* earned Trithemius the accusations of demonology. The third book included discussions of spirits and planetary intelligences, and remained undeciphered and unexplained well into the twentieth century. Even Shumaker's work, published in 1982, had to make due with a guess about the "true" contents of the mysterious third book.

But then, in the late 1990s, two scholars independently "cracked" the third book of the *Steganographia*, showing how, like the first two books, despite vivid discussions of spirits and planetary intelligences, there is a real use of cryptography (putting to rest the accusations, according to these authors, that Trithemius had any demonological intentions).[81] The third book contains eight tables of numbers, grouped by the names of twenty-one planetary spirits or "rulers," in which each column contained data necessary for computing the position of a specific planet (see Figure 3.5). To communicate secretly and swiftly without using human messengers, but by "natural" means (Trithemius insists), one must first use the data in the table to calculate the position and course of the appropriate planet. Then an image of the appropriate spirit is drawn on one piece of paper, along with the name of the recipient, and on another piece of paper the process is repeated, replacing the recipient's name with the message to be transmitted. The message itself must not violate a number of prescribed rules—the message must be of a loftiness of purpose, and cannot suffer from lack of clarity. Trithemius stated that the correct notation, or "character," must be used to attract the appropriate spirit, otherwise the spirit

[80] Ibid., 104.
[81] Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia"; Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia."

may "refuse to obey."[82] This requires, above all, identifying the correct astrological sign. Once the entire process is complete, both sheets are brought together and placed in a special box, and within twenty-four hours the recipient will receive the message. Other sequences and descriptions in the third book can be decrypted in a manner similar to the first two books.[83]

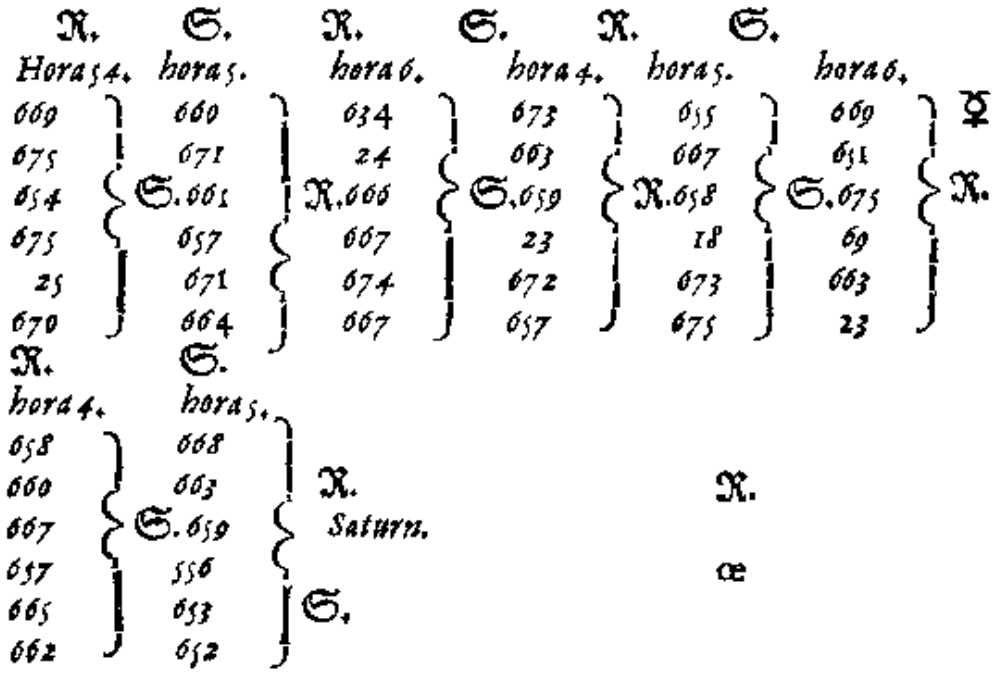


Figure 3.5: Codes for invoking the Angel of Saturn, from book three, table three of Trithemius' *Steganographia*.[84]

With these fabulous descriptions of communication aided by spirits, many scholars believed that the third book did not contain any cryptographic content, and was instead purely demonological. The most authoritative modern voice holding this position was D.P. Walker in his *Spiritical and Demonic Magic from Ficino to Campanella*. Similarly, Nicholas H. Clullee claimed in his book, *John Dee's Natural Philosophy Between Science and Religion,* that there could not be any cryptography in the *Steganographia's* third book because it would be a

[82] Brann, *Trithemius and Magical Theology*, 138.
[83] Both Ernst and Reeds offer descriptions of the decryption process, in addition to their personal account of cracking the code; Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia"; Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia."
[84] Trithemius, *Steganographia (Secret Writing)*.

conceptually unnecessary addition, since Trithemius indicated that the spirits transmit the messages "directly." Ernst and Reeds showed that it does contain cryptography, but, I argue, this does not mean that it renders the spiritual exercises useless or excludes them, as they suggested.

The spirits and planetary intelligences have an important function, they draw the mind away from changing particulars and towards universals. For example, in Agrippa's *De occulta philosophia*, a product of Trithemius' counsel, his method is analogous in that it is intended to "proceed towards high things" and turn the mind "confidently to universals."[85] To gain true knowledge one must investigate occult ("hidden") resemblances using an appropriate method, aided by magic and spirits.

The spiritual exercises of the third book of the *Steganographia* reveal certain knowledge and enable communication through the web of resemblances, enfolding the human and divine universes within. In order to move past sense perception alone, magic and assistance from spirits were required, and therefore inextricably linked to scholarship. For miraculous phenomena—which all people in the sixteenth century believed in—the senses alone were especially insufficient for attaining knowledge. For communication, on the other hand, transmitting messages at a distance, without an intermediating material body (in many cases a literal messenger was the typical communication media), was understood to be possible only with the assistance of mediating spirits. Epistemology and technical communication together hinge on the resemblances of *aemulatio*: working at a distance without motion, and free from place.

The other kinds of resemblances also played important roles in Trithemius' cryptography. Analogy was critical for Trithemius' paper-based media scheme, which required drawing images of planetary beings, who would aid in communication. In fact, analogy is a superimposition of *convenientia* and *aemulatio,* and a reconfiguration of the old processes of mimesis. By drawing a planetary intelligence (which can be a rough sketch, and reused for other messages, according to Trithemius),[86] analogy worked as a kind of mirror between the drawn image and the intended recipient's mind.

The resemblance of sympathy is perhaps the most pervasive through Trithemius' technical communication schemes. Trithemius suggested that

[85] Shumaker, *Renaissance Curiosa*, 109.
[86] Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia," 323.

appropriately prepared lodestones, ringed with letters akin to a cipher wheel,[87] could transmit instantly across vast distances through sympathetic qualities interior to the lodestones. Similarly, Trithemius reported, after two people rub together the blood from cuts on their arms, they will be able to communicate through sympathetic pin pricks, a kind of global vascular Morse code.

While Ernst and Reeds have unequivocally proven that the third book of the *Steganographia* contains a form of cryptography, it is not the case that the invocations of spirits and planetary intelligences have nothing to do with Trithemius' cryptography; nor do their findings mean that Trithemius' claims of using only "natural" means for communication is exclusive of cryptographic processes (nor imply he was lying).[88]

The key to understanding why Trithemius invoked spirits, and yet insisted that he did so "naturally," is to be found in his understanding of nature, which implicitly recognized the category of preternatural. For sixteenth century occultists like Trithemius, nature was not a binary of the supernatural and natural. Rather, as Daston has argued, there is a third category of being, called preternatural, that was technically part of nature, but occupied by higher *created* beings, such as angels and spirits.[89] The origins of the theory of preternatural being, according to Daston, is found in Augustine's conception of nature, who believed that all created beings stem directly from God. On the Augustinian view, all nature, but especially the miraculous, was supernatural. Aquinas later altered Augustine's view, arguing that within nature there is a distinction to be made between the natural that occurs with regularity and order, and the natural that occasionally occurs. Miracles may be strictly outside of the understanding of humans, and thus belong properly to the supernatural world, but other unusual phenomena may be the result of natural processes. Marvels and the actions of spirits, for example, occur rarely, but are the result of created beings and thus, can be understood by humans (with difficulty). That is, spirits are *created*, but *special,* beings—they are "preternatural." So, as Trithemius insisted,

[87] See also Brann, *Trithemius and Magical Theology*, 145.

[88] Reeds writes that "the cryptographic techniques are purely natural" and are only "disguised by the use of a figurative language of demonology," and that "the *Steganographia* can no longer be regarded as one of the main early modern demonological treatises but instead stands unambiguously revealed as the first book-length treatment of cryptography in Europe." Ernst appears to be much more careful about recognizing the historical context in which Trithemius was writing, noting that spirits and fabulous media technologies were commonplace and, in the minds of the authors of the day, necessarily part of cryptography. Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia."

[89] Daston, "Marvelous Facts and Miraculous Evidence in Early Modern Europe."

invoking spirits to assist with cryptographical activities was still "[preter]natural," and not supernatural.

Trithemius' designs for technical communication might have surpassed the limitations of material communication, but he did believe they worked by impossible means, or escape the need for a medium. Without a medium, communication would be impossible but, a typical material medium is obviously not fit for the task Trithemius requires of it, so he invents a more capable medium. Here, spirits perform the necessary mediatic role, bridging the gap between plaintext and ciphertext, or source and destination.

The transmission process also extends writing, here used as a technical medium, as it requires special performances and careful calculations. Trithemius suggested that these special performances and calculations are a part of grammar. And, this special part of grammar is not outside of writing, but rather a refinement and extension of writing.

3.3 Type, Notation, and Plaintext

By the end of the fifteenth century, mimetic technologies and their processes were changing, as new and emerging technologies for communication, calculation, and memory took their places. Here, at this intersection, Alberti's cryptographic innovations emerged. Alberti's cryptographic and architectural work broke new ground by inaugurating a notational epoch—with new logics of order, composition, and ways of representing. These new logics were influenced by the invention of the movable type press, which functioned as a kind of prototype for Alberti's innovations in cryptography. In contrast to the relatively static movable type press, Alberti's cipher wheel (and his architectural plotting device, which I describe below), were dynamic technologies that enabled, as we might say today, "data driven" and "algorithmic" approaches to representation and communication.

Alberti was able to break new ground because his approach to the methods and designs were relatively free from old mimetic thinking. For example, when describing his cipher wheel, Alberti referenced the ancient *loci* method of memory arts in a Lullian, notational style, rather than the imagistic style introduced by Aquinas. Or, for example, in his architectural work, *De re aedificatoria,* Alberti formalized ancient architecture without mimetic illustration, or even, written description. In fact, according to Carpo's assessment of Alberti's architectural corpus, there were no drawings of ancient monuments, nor even written reconstructions of any buildings; instead Alberti supplied *rules* for all'antica construction. However, Alberti was less thorough in

his other works. For example, Alberti still used mimetic descriptions for his theories of painting and the plastic arts.

It was only in late modernity, perhaps with Leibniz, when the project that Alberti started was fully realized, as code became properly notational.[90]

3.3.1 The printing press as prototype for a notational epoch

Returning to this chapter's initial provocation, what role did the invention of the movable type press have on Alberti's thinking, and how did this lead to a "new species" of cryptography and the dawn of a notational epoch? First, movable type was invented in Alberti's lifetime and was influential for him. Carpo calls Alberti the first "typographical architect,"[91] and the same can be said for his cryptographic work, built from Lull's notational, combinatorial wheels. For Alberti, the invention of movable type highlighted reproducible, modular, indexical, and combinatory logics. While the invention of the alphabet brought forth the necessary identity requirements for writing to become plaintext, it was, however, the movable type press that made the analytical aspects underneath the machinery clear and apparent.[92] Kittler wrote that printed *books* share with computing technologies (and cryptography) "the deep quality of being discrete media," that is, they are both notational media.[93] In the same way that later computers and calculation machines would be defined by their notation, Alberti put these typographic logics to *work*.

Far from only affecting the way words land on a page, the moveable type press changed existing notions of reproducibility. Alberti was familiar with the idea of reproducing identical copies from woodcuts, a pre-Gutenberg technique now called xylography.[94] But, Xylography produced whole "images," typically an etched picture, and sometimes the reproduction of a complete page, which included textual elements. Entire books—texts and images together—could be printed using xylographic processes, but this "block book" process was rare and may have even originated *after* Gutenberg's invention, as a quick and cheap alternative to movable type. More to the point, printing from woodcuts, while possible, had serious limitations. Because each successive "edition" introduced the chance of error, block book production was poorly suited for technical

[90] See chapter ten for a discussion of Leibniz's calculation and cryptography machines.
[91] Carpo, *The Alphabet and the Algorithm*.
[92] These logics were also apparent in later cryptography manuals; see Ellison's analysis of John Falconer's combinatory logic: she also argues that many of these functional aspects originally inhered in the alphabet. Ellison, "'114400072777607680000 Wayes'" para. 27.
[93] Kittler quoted in Ernst, *Digital Memory and the Archive*, 117.
[94] Carpo, *Architecture in the Age of Printing*.

works of the sort Alberti was interested in.[95] In fact, the chance of copyist error for pictures was so high that authors typically wrote *textual* (ekphrastic) descriptions instead, for what are fundamentally visual phenomena, such as architectural plans and forms.[96] Alberti was so worried about errors in his architectural works, that he requested copyists write out numerals in longhand, rather than using numeral symbols.[97]

Avoiding the introduction of errors was one of the principle advantages of type for the reproduction of technical works. Traditionally, manuscripts were produced by scribes taking dictation. Scribes could be counted on to (somewhat) reliably replicate the correct order of a determinate set of icons (the alphabet or Arabic numerals), but technical images and diagrams would have proven nearly impossible. Moreover, natural language is highly redundant, which permits some degree of error. Etched woodblocks, on the other hand, would help to ensure exact duplication for images, so long as the etching was correct, but these tended to get worn and broken over time.[98] For manuscripts, duplicating a technical image is to invite critical mistakes.

Error propagation is also a real concern for cryptography. Polyalphabetic encryption "mixes" multiple alphabets with plaintext, which results in a kind of "diffuse" ciphertext. For any one letter of plaintext, the corresponding ciphertext might be several letters, or letters mixed about in unpredictable ways. For cryptography, redundancy is, ideally, non-existent in ciphertext. Anticipating his later work on entropy and information, Shannon recognized that cryptographic "diffusion" and "confusion" techniques are basic methods of reducing redundancy, which frustrates cryptanalytic techniques by "hiding" plaintext more deeply within a combinatory space.[99] The result, highly diffuse ciphertext (typically understood as "good" cryptography), makes for very "brittle" transmission. Even a small copying or transcription error might render much or all of the resulting ciphertext impossible to decrypt. Very careful

[95] The same problem plagued Francesco di Giorgio in the fifteenth century, whose technical drawings of hoisting cranes became so corrupt a century later that, due to the omission of key elements (such as a working block-and-tackle system), his inventions were for all practical purposes lost. It may have been the case that some errors could be "fixed" on interpretation by a master builder already familiar with the working principles, but to those truly novel designs such errors would prove ruinous. See Misa, *Leonardo to the Internet*, 27.

[96] Carpo, *Architecture in the Age of Printing*, 18; Eisenstein, *The Printing Press as an Agent of Change*, 47.

[97] Writing numbers in textual longhand has the advantage of linguistic redundancy. See Carpo, *Architecture in the Age of Printing*, 119.

[98] Eisenstein, *The Printing Press as an Agent of Change*, 53.

[99] Shannon, "Communication Theory of Secrecy Systems."

transcription, or error-correction codes (as we use today) are a practical necessity for even moderately strong cryptography.[100]

Modularity was one of the byproducts of the introduction of movable type. Creating manuscripts by hand required the inscription of letters *in situ* (and at the time of production). On a printed page, however, letters pre-exist as units of type before the creation of words in which they occur. Explaining the influence of movable type on modularity, Harris writes, "mechanical regularity of print confers upon each alphabetical symbol an independence and a constant visual identity which no earlier form of writing quite achieves."[101] In Alberti's work, the letter became a metaphor for modularity, suggesting that the architectural form or ciphertext could be assembled, just like a word created from its constitutive letters. That is, the invention of the movable type press transformed letters from icons in the imagination to fungible materials. With the movable type press it became clear to everyone involved that individual letters (in the form of literal pieces of metal) (see Figure 3.6), were distinct, yet produced identical inked impressions. One consequence of this change was that the letter, not the page, became the locus of identity. Ong argues that the invention of movable type much more strongly implied a sense of modularity than the written alphabet.[102] According to Ong, the "discrete" letterforms of the printing press were modular and interchangeable, and since written letters had long stood as symbols, the entire system became a modular form of symbol manipulation.

[100] See also Shumaker, who argues that "Copyists—and typesetters—who must toilsomely reproduce long stretches of letters that make no sense to them are peculiarly liable to error;" *Renaissance Curiosa*, 100.
[101] Harris, *The Origin of Writing*, 7. For a similar notion, called "decontextualization" see Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*.
[102] Ong, *Orality and Literacy*.

Figure 3.6: Setting type in a print shop, from plate 5 of *Nova Reperta* (c. 1600).[103]

As print suggested that letters are things, letters came to be more strongly indexical.[104] By "indexical," I mean the ways that printed letters narrowly referred to, or "indexed," their alphabetic signifieds. That is, letters came to more obviously link symbol to signified, a transitive form of identity. In fact, the transitive link of letters in these new systems was so strong as to surpass their former role as symbols, which usually have a fungible variability. Symbols are powerful precisely because they can be reused and altered (any given symbol can, in theory, stand for something else). By making letters concrete, they became more indexical, which made it easier to see how letters could stand in for more abstract or ethereal things. So, letters were understood to aid in the combination and analysis of many matters. For cryptography, as we will see, substituted letters for a particular encryption event hold an iron-clad transitivity, linking plaintext and ciphertext in ways that can never be broken

[103] Stradanus, *Nova Reperta* c. 1600. (1948,0410.4.194, AN148253600l). http://www.britishmuseum.org/research/collection_online/collection_object_details.aspx?objectId=1609177&partId=1&searchText=Nova+Reperta&page=1. Image licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) license.

[104] Ong, *Orality and Literacy*, 116.

apart (e.g., see below, how <A> → <G>). If this transitivity is lost, decryption becomes impossible.

According to Carpo, Alberti sought "indexical sameness," *and* had a "quest for identical replication."[105] Herein lies a problem of interpretation. While indexical sameness is an operation of transitive identity, identical replication is a visual operation based on mimetic similitude. The difference between a block book and movable type book offers an example of the distinction between indexical sameness and identical replication: the xylographic (block) printing press certainly did create visually identical books—identical pages neatly organized and bound together to create a unified whole. Furthermore, identical replication of books resulted in important social and bibliographical patterns of change.[106] However, identical replication does not explain the impact the movable type press had on Alberti's thinking. It was, rather, *movable* type, with individual and (re)combinable letters, that made the new forms of indexical identity possible, and thus played such an important role in Alberti's thinking.

The invention of letters, and then the printing press, also suggested a new combinatory way of thinking. The novelty of printing from movable type would have drawn attention to the combinatory logic inherent in the alphabet.[107] For a while, combinatorial thinking was even turned into a practical method. For instance, in his *Dissertatio,* Leibniz developed a method for investigating new relationships called "*ars combinatorial.*"[108] In this early work, Leibniz suggested that combining letters and interrogating their resulting configurations, which he called "complexions," could explore all aspects of reality. Each complexion could be organized into a table or run through a calculating (or even cryptographic) mechanism—creating atomic parts that reveal orders and local relationships, much like computers today.[109] Such an activity *combines* existing facts in new and surprising ways, revealing hidden order that might not have been apparent to the unassisted eye (or creating hidden order, that is not apparent to the unassisted eye). In fact, we can think of Leibniz's machines as part of the long tradition of using the alphabet—actual notation—in really unusual ways, that is, for communication and calculation.

---

[105] Carpo, *The Alphabet and the Algorithm*, 28.
[106] In many cases, however, printed books remained *sui generis* due to individual differences in production. See also Eisenstein, *The Printing Press as an Agent of Change*, 49 ff.
[107] Carpo, *Architecture in the Age of Printing*, 54.
[108] Leibniz, *Dissertatio de Arte Combinatoria*. An English translation is available in Leibniz, "Dissertation on the Art of Combinations." See chapter ten for a description of Leibniz's cryptographic work.
[109] See chapter ten for a description of Leibniz's calculating machines and their use in cryptography.

3.3.1.1 THE PERSISTENCE OF MIMESIS

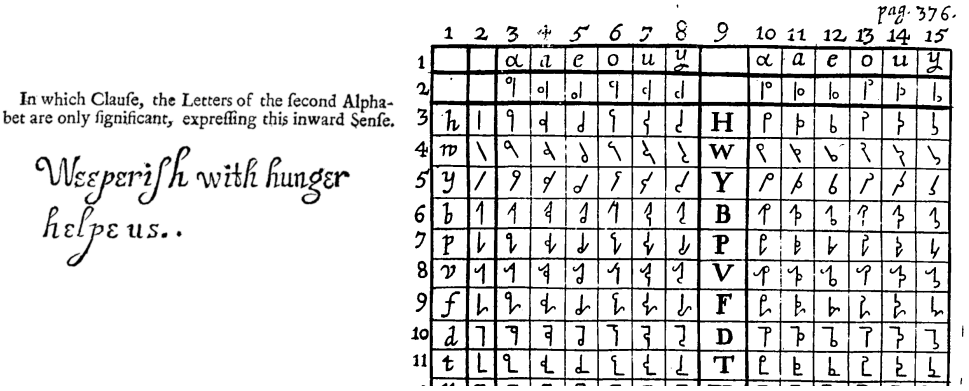
So, what is new here? The movable type press is, after all, just a mechanism for organizing letters on a printed page, and letters have been around for more than three millennia. The moveable type press did not introduce new ontologies through its use (the letter did),[110] but the movable type press did make such logics more apparent and obvious. Despite the advances made in notational technologies, mimetic approaches still played a significant role in new and emerging media.

Against this linear development towards more highly refined and abstract notational characters, in some cases cryptographic ideas outpaced available technology. Due to the orthographic complexities of some code systems, the movable type press actually fused with notational technologies, resulting in what Ellison calls "multimodal" production.[111] Multimodal production is the result of the need to add manual inscriptions to printed letterforms because of the technical inadequacies of printing from movable type. In fact, multimodal production resulted in a s*ynthesis* of type and manuscript, lasting for several centuries past the invention of the "superior" technology of moveable type.[112] For example, John Wilkins' complex schemes for perfect languages and ciphers in *Mercury,* and his *Essay,* required manual additions to the typescript (see Figures 3.8 and 3.9). The analytics of Wilkins' complex code simply outstripped the capabilities of the reproduction technologies of the time.

[110] Note that, in accordance to the archeological method I set out in the Introduction, the invention of the letter really did bring something new into the world through its use. The movable type press was a refinement of the underlying schema made available with the earlier invention.

[111] Ellison, "Millions of Millions of Distinct Orders."

[112] See Eisenstein, *The Printing Press as an Agent of Change* for an in-depth assessment of the slow replacement of manuscript production, occurring in fits and starts and regressions, on account of the invention of the printing press.



In which Clauſe, the Letters of the ſecond Alphabet are only ſignificant, expreſſing this inward Senſe.

Weeperiſh with hunger
helpe us..

pag. 376.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1			α	a	e	o	u	y		α	a	e	o	u	y
2			٩	٥	٥	٩	٤	٤		١٥	٥	٥	١٥	٥	٥
3	h	l	٩	٩	٤	٩	٤	٤	H	٩	٥	٥	٩	٥	٥
4	w	\	٩	٩	٥	٩	٤	٤	W	٩	٥	٥	٩	٥	٥
5	y	/	٩	٩	٤	٩	٤	٤	Y	٩	٥	٥	٩	٥	٥
6	b	٦	٦	٩	٤	٦	٩	٩	B	٩	٥	٥	٩	٥	٥
7	p	٥	٩	٩	٤	٥	٩	٤	P	٩	٥	٥	٩	٥	٥
8	v	٦	٦	٩	٤	٦	٩	٩	V	٩	٥	٥	٩	٥	٥
9	f	٥	٩	٩	٤	٥	٩	٤	F	٩	٥	٥	٩	٥	٥
10	d	٦	٩	٩	٤	٦	٩	٤	D	٩	٥	٥	٩	٥	٥
11	t	٥	٩	٩	٤	٥	٩	٤	T	٩	٥	٥	٩	٥	٥

Figures 3.7 and 3.8: (left) Detail of stenographic writing from print edition of *Mercury* (1641); (right) Detail of sound alphabet from print edition of *Essay* (1668), both showing evidence of multimodal production.[113]

3.3.2 Alberti: Notation and plaintext

When developing new "writing" technologies, Alberti seemed to understand the ways that his inventions required new thinking about knowledge and communication. In such cases, Alberti would often replace discussion of mimetic forms of representation with notational ones.

In the *Descriptio Urbis Romae* (Figure 3.10), Alberti developed an ingenious device to plot the coordinates for a plan of Rome. Avoiding issues involved in scientific and engineering communication that use mimetic, visual descriptions, and the potential errors these methods introduce (as discussed above), Alberti's "reconstruction of Rome" works by listing the coordinates of points, which are then plotted with a ruler pinned to the center of a circular horizon. By matching notations on the ruler to notations along the circumference of the horizon, the user can recreate the plan of Rome—first, plotting the points, and then, in a kind of "connect-the-dots" way, drawing the outline of the plan. Carpo calls Alberti's invention a way of producing "digital images."[114] When his plotting machine (hardware) is combined with the appropriate method (software) and fed suitable coordinates (data) it produces images. Alberti also enlarged the scope of the mechanism in *De statua,* for use in three dimensions, as a way to re-present the human body.[115]

[113] Wilkins, *Mercury: Or the Secret and Swift Messenger*, 38; Wilkins, *Essay Towards a Real Character and a Philosophical Language*, 396.
[114] Carpo, *Architecture in the Age of Printing*, 123.
[115] Ibid., 122. Carpo notes that "the key piece of hardware in Alberti's *De statua* was a revolving instrument, a wheel of sorts, in this case somehow inconveniently nailed to the head of the body to be scanned" Carpo, *The Alphabet and the Algorithm*, 55. *De statua* regresses to mimetic

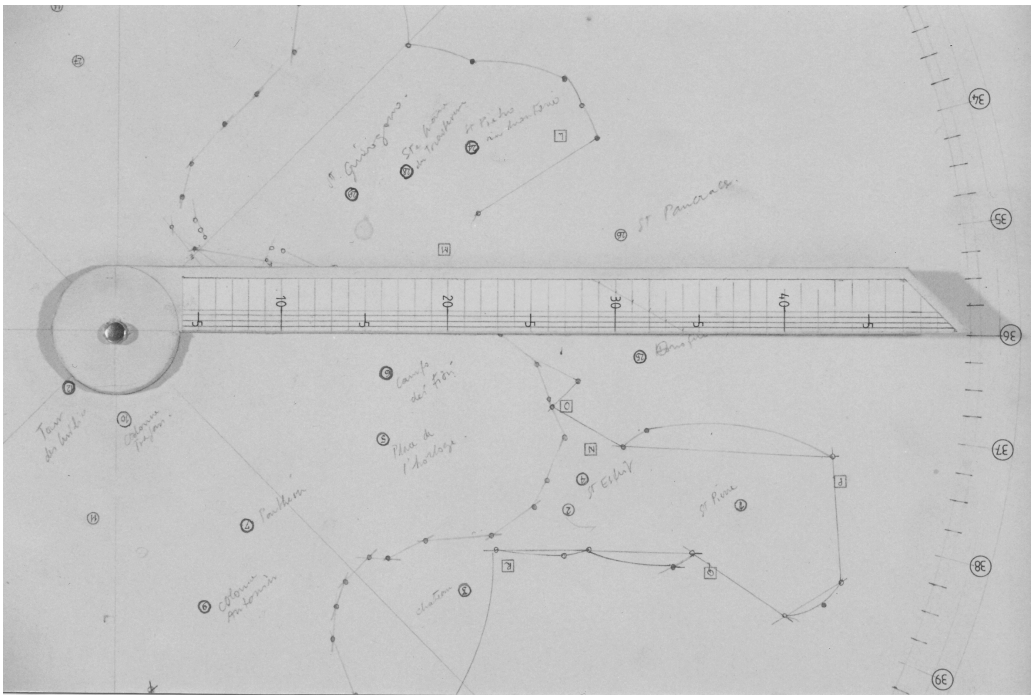


Figure 3.9: Reconstruction of Alberti's *Descriptio Urbis Romae* (c.1433) *mechanism.*[116]

There are interesting and significant parallels between Alberti's mechanism for architectural plans in the *Descriptio* and his cryptographic invention in *De Cifris*.[117] The latter presents a method and mechanism for polyalphabetic encryption using a cipher wheel, which Alberti described as being composed of two rotating, circular planes that are attached to a center pin or string around which they rotate (Figure 3.11). The disk is divided "into twenty-four coequal parts; these parts of the circle are called houses."[118] Upon each rotation of the disk, a new indexical relationship (a "key") is established. The cryptographic "key" is set by aligning two letters; Alberti wrote: "say such k lies under the upper-case B."[119] To encrypt a message, the user substitutes each letter of the

explanations, however, as Alberti envisions the task of the sculpture to be a mimetic representation.

[116] Reconstruction by Bruno Queysanne and Patrick Thépot. Image used with permission by Patrick Thépot.

[117] Kahn does not believe that Alberti's *Descriptio Urbis Romae* device has a historical connection to the cipher wheel, however for my purposes there is certainly an archeological connection, and I suspect, a historical connection as well. Kahn, "On the Origin of Polyalphabetic Substitution."

[118] Alberti, "De Componendis Cifris," 181 (xiii).

[119] Ibid. (xiv)

plaintext to its "twin" along the other plane, and to decrypt, the process is reversed.

Figure 3.10: The rotating horizons of Alberti's cipher wheel and attached by string, from *De cifris* (1466).[120]

Alberti describes the transformation using an example: "[t]hus a common letter, say A, will take on the meaning of another letter, say G…."[121] If Alberti's desire to print *De cifris* on a moveable type press had been realized, the transformation of <A> to <G> would in no way have been metaphorical. With movable type, an <A> can be literally replaced with a <G>. From the *material* of movable type to the *real* of cryptography, <A> → <G> is an indexical substitution. The relationship is indexical because <A> specifies, or points to, <G> in a rigorously univocal and unchanging way. Moreover, each letter's self-identity is also required, but it need not be a relationship of resemblance (<A> = <*A*> = <a>, and so on). On the other hand, there must be an in-principle way of determining the difference between <A> and <G>. Crucially, the link

[120] Alberti, De componendis cifris. Image licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license (Buonafalce, https://commons.wikimedia.org/wiki/File:Alberti_cipher_disk.JPG).

[121] Alberti, "De Componendis Cifris," 179. "Itaque aut usitate littera uti est .a. aliam quampiam significabit, ut puta .g. et littera .b." in Meister, *Die Geheimschrift Im Dienste Der Päpstlichen Kurie von Ihren Anfängen Bis Zum Ende Des XVI Jahrhunderts*, 134. It should also be noted that I call the essential cryptographic property "substitution" instead of "substitution or transposition." I take transposition to be a species of substitution (substitution within a set).

between plaintext (<A>) and ciphertext (<G>) must not be altered for the entirety of the process. The whole system works as long as any given thing, natural language or otherwise, can be broken into letters of plaintext, which, when encrypted, maintain an indexical relationship between plaintext and ciphertext.

The cipher wheel orders the written world "digitally," just like the plotting device in the *Descriptio*. Alberti's cipher wheel capitalizes on the way that words can be decomposed into modular, discrete things. That is, Alberti's cipher wheel *uses* features of natural languages, the particular identity requirements and redundancies, as the raw material to be re-ordered for the process of encryption. Each language, and each form of expression, has its own essential characteristics, which can be either perfectly transcribed/encrypted or imperfectly translated. For instance, language translation works *with* properties that are essential to the expression—attempting to maintain the essential characteristic from the original in the translated version. Practically (and perhaps essentially), there is always a certain parallax between source and target translations, as some shades of meaning or quirks of syntax fail to get translated. Similarly, when using Alberti's *Descriptio* mechanism to convert the plan of Rome, from a mimetic or "real" representation into a digital version, many characteristics of the plan are abstracted, altered, or ignored.

Unlike translation, Alberti's encryption cipher uses the essential qualities of language to its advantage, working on the level of what he calls "natural" syntaxes. The process of encryption relates the intrinsic qualities[122] of letter "orders" to "numeric ratios,"[123] that naturally form vowels and consonants, bigrams and trigrams.[124] Unlike translation, which attempts to use "natural" syntaxes to link source and object languages as best it can, ciphers use these features against the effable, publically shared, and "natural" aspects of the language itself.[125]

In language, Alberti writes, syntaxes (or identities) are already naturally "scrambled" about. To encrypt a message, a cryptographer must act like a dutiful caretaker, collecting leaves blowing in the wind. The process of encryption then rakes the leaves into piles, forcing artificial identities and orders.[126] Similarly, Alberti describes the cryptographic process as one that

[122] "De notis literarris quales sese natura" (iv).
[123] "numeri rationibus" (iv).
[124] See Alberti, "De Componendis Cifris," 173–78.
[125] See chapter nine for a description of the distinction between translation and encryption.
[126] Alberti, "De Componendis Cifris," 179 (xi). Della Porta also discusses the "dislocations of the natural order of letters," see Shumaker, *Renaissance Curiosa*, 116.

places individual letters into "houses"[127] (recall Quintilian's method of placing items in mental "houses" in the *loci* method); the smaller wheel of the cipher contains "mobile" houses. Together, the two wheels are a formula,[128] where the relative positions of the houses (the "index") are like a "key." The process is only possible when the totality of the system is present, that is, all of the parts of language must be stored in the houses, and their relative positions adjusted and remembered (or written down).

In the above description, Alberti's cipher wheel is nothing more than a handy mechanism for common substitution ciphers (known since antiquity as a "Caesar" cipher). Alberti's real innovation, however, is the way that he incorporates multiple alphabets to form polyalphabetic encryption—he writes, "after I have written three or four words I will mutate the position of the index in our formula, rotating the disk let's say, so that the index k falls below the upper-case R."[129] By rotating the disk during the process of encryption a "new" alphabet is introduced with each turn, making cryptanalysis significantly more difficult by increasing the combinatory space of the ciphertext.

In hindsight, a theory of technical communication necessary to explain the functioning of Alberti's machines would not develop until the twentieth century, and a description of the notational discourse network he was working within is still wanting. This lack of suitable conceptual and technical explanation, about how notational technologies really worked, produced a palpable reticence for those engaged in engineering and scientific communication. The "pretypographical architect knew that for… long-distance transmission," Carpo offers, "images were not a trustworthy medium… and he practiced his craft within these limitations."[130] Moreover, in the quattrocento, there was a rapid expansion of economic, diplomatic, and scientific commerce, and new, long-distance transmission of materials, of many types, became vitally important alongside the demands for secret diplomatic communication. To satisfy this need, Alberti argued, cryptography is needed—which has to be secret, capable of long-distance transmission, and, above all, efficient (Alberti called it "commodious" [*scribetur commodius*]).[131] Such demands for communication are as apparent today as they were for Alberti.

With his novel techniques and designs that work without reference to mimesis, Alberti's work can be understood as innovative in that it rails against

[127] "hae partes domicilia nuncupantur" (xii).
[128] "formulam."
[129] Alberti, "De Componendis Cifris," 181.
[130] Carpo, *Architecture in the Age of Printing*, 29.
[131] Alberti, "De Componendis Cifris," 180. (xii).

ancient methods of representation, communication, and transmission. Alberti's work also ushered in a method for mass production. Carpo notes that in Alberti's world of handicraft, "imitation and visual similarity were the norm, replication and visual identicality were the exception."[132] Just as Alberti's architectural methods gave rise to "designed" buildings—in distinction to the old handicraft of architecture that existed before him—his cryptographic methods ushered in new kinds of indexical writing. That is to say, Alberti developed notions of indexical sameness, and not *identical* sameness (as in mass production, where each piece resembles the others). Alberti's mediatic methods were powerful because they offered the right kinds of sameness, and also permitted modular adjustment and reordering. Individual letters, printed from movable type presses, provided the prototype from which Alberti developed his notational machines, used in architecture and cryptography.

Alberti's advances towards a notational form of architecture would be, in fact, rolled back in significant ways. The introduction of powerful computers in the twentieth century, working directly with an inner (binary) notation, would, nonetheless, find frequent use in visual design—an ancient, mimetic, even "painterly" form of expression. Today, most CAD programs are thoroughly mimetic, and it is only at the fringe of artistic and experimental practices that algorithms are used *directly*.[133]

Alberti's cryptographic work fared somewhat better, at least in the long run. Leibniz organized and theorized the ways that notation can be put to work, and provided an analysis of order necessary for understanding cryptography. Then, in the twentieth century, Shannon excluded whatever faint notions of resemblances were left, dismissing *de jure* all aspects of meaning and psychological difference. In practical terms, mimetic theory no longer has much relevance in the field of cryptology, as engineers and cryptographers today produce products that, at the very least, appear mathematical. Despite the orientation of engineers, for scholars interested in understanding the role of cryptography in society, insufficient attention has been paid to the ways notation—and not mimesis—configures media and cryptography.

❦

The development of the notational epoch arises from a long changing history of mimetic theory. The first signs of change begin to show in the late Middle Ages. In the thirteenth century, Lull's volvelles influenced Alberti, who

[132] Carpo, *The Alphabet and the Algorithm*, 3.
[133] Algorithms are used extensively throughout modern computing, but rarely do we interact with them directly, and I see this as a problem.

developed a cipher wheel in the fifteenth century. The invention of the movable type press was also an important prototype for this new kind of notational thinking. Trithemius and many other cryptographers, however, still sought solutions in the power of hidden resemblances. To understand the critical point that resemblance played in this narrative, it is worth quoting Foucault's commentary at length:

> *Up to the end of the sixteenth century, resemblance played a constructive role in the knowledge of Western culture. It was resemblance that largely guided exegesis and the interpretation of texts; it was resemblance that organized the play of symbols, made possible knowledge of things visible and invisible, and controlled the art of representing them. The universe was folded in upon itself… And representation–whether in the service of pleasure or of knowledge–was posited as a form of repetition….*[134]

Indeed, everything changes at the end of the sixteenth century. Francis Bacon developed a simple and rather forgettable cipher in his youth, but the cryptographic idea appears to have planted a seed for a new scientific topic and a new direction for the use and development of language. Within a few decades, Bacon developed a proposal for an artificial language of vast power, with properties strikingly similar to the goals of cryptographers prior to him—a notational medium capable of spanning place and time, solving the challenges of science, and ultimately bringing all of humankind back under a single language. Developing an artificial language to solve these representational issues would stir the greatest minds of the next two centuries, and cryptography played an important role in the development of this new medium.

[134] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, 19.

4
Language planning in the sixteenth and seventeenth centuries

"Words are the images of cogitations," writes Aristotle, "and letters are the images of words." But in his 1605 *Advancement of Learning*, Francis Bacon (1561 – 1623) rebuts Aristotle's claim: "it is not of necessity that cogitations be expressed by the *medium* of words."[1] Bacon's critique of the Aristotelian theory of language was motivated by his belief that natural languages, either written or spoken, are inherently illusory. According to Bacon, words in natural languages mimetically represent a world of personal bias and false belief, and therefore lead to the breakdown of communication and the obstruction of scientific progress. The only way to correct the corrupting effects of natural language, a necessary activity for scientific advancement, was to design a form of communication that is faster, more accurate, and more precise. Bacon had two interrelated plans for his new communications medium: a "Real Character" capable of representing the essences of things, and a "bi-literal" cipher capable of representing "anything by anything." Thus, Bacon argued, the "medium of words" should be replaced by a "new" medium, one that is artificial, universal, and perfect.[2] As these investigations gained popularity, the language planners that followed Bacon's early designs drew from the same kinds of cryptographical resources for the development of their artificial languages.

In this chapter, I draw out the historical and conceptual connections between artificial language planning and cryptography. I argue that the two topics are historically related. Artificial languages, together with cryptography, were

[1] Bacon, "The Advancement of Learning," 230. All references to *Advancement of Learning* are to Vicker's modern version, unless otherwise noted. In general, Vicker's version is a light modernization of Bacon's 1605 *The two bookes of Sr. Francis Bacon. Of the proficience and aduancement of learning, divine and hvmane, reprinted in 1629 as The Two Bookes of Sr. Francis Bacon. Of the Proficience and Aduancement of Learning, Divine and Hvmane*. This work was heavily expanded into a Latin version titled *De Augmentis Scientiarum*, and also translated into an English version by Gilbert Wats in 1674; for English translations of this work I am using Bacon, "Translation of the 'De Augmentis.'" The Latin work is crucial to the discussion of cryptography, since the original *Advancement of Learning* includes only a very short discussion of cryptography, omitting Bacon's bi-literal cipher entirely.

[2] There are many different formulations for proposed languages during the sixteenth and seventeenth centuries, each with a different focus and approach, including attempts to rekindle a pre-Babel language, designs for languages with universal aspirations, or designs for languages that attempt to be sufficient for science in its perfection and philosophical acuity.

thought to be useful for the reformation of scientific method, as a method to return to prelapsarian linguistic purity, and as a system of pure and perfect communication. Moreover, there are numerous shared conceptual features between artificial languages and cryptography, including the use of notation for precise and unambiguous representation, efficient communication, and the combination of things. That is, artificial languages of the sort planned throughout the sixteenth and seventeenth centuries have a range of historical and conceptual interconnections with the development of cryptography.

This chapter extends the argument developed in chapter three, that plaintext is a form of writing, and historically, was connected with such investigations. This chapter also focuses on the ways that plaintext was used for investigating the natural world, as a kind of data-driven proto-computer. Whereas chapter three focused on the deployment of the logics of identity and combination in typography and the moveable type press, this chapter focuses on plaintext's relationship to language. As such, this chapter can be read alongside chapter nine, where I argue that the encryption/decryption process is a form of transcription and not translation. Encryption is not a linguistic process.

The distinction between written language and plaintext is often seemingly without difference. A written English word, for example, may be *simultaneously* linguistically comprehensible and functional to readers (natural language), while also potentially encrypted (plaintext). Other inscriptions, however, may function linguistically but are not suitable as plaintext, as for instance, Chinese logographs.[3] Artificial languages of the sort described here, therefore, may sometimes function as a kind of code, spanning between meaningful writing and plaintext. In fact, the more elaborate artificial languages of this era, end up looking a lot like a form of cryptography, and may not even function particularly well for linguistic purposes. Nonetheless, there is no hard and fast division between those systems that are linguistic, and those that are cryptographic. Given these shared conceptual lineages, it is not surprising that the histories of plaintext and artificial language planning co-developed.

The search for artificial languages that swept early modernity was in large part due to growing scientific naturalism, inaugurating what Foucault later called the taxonomic *episteme* (*taxinomia*).[4] The taxonomic *episteme* was rooted in Aristotelian classification and takes seriously the possibility that there is no separation between naming and defining. Foucault calls this "a set of essential

[3] This is not to say that Chinese writing cannot be encrypted, but rather, that it cannot be encrypted as a logograph. See chapter five for more details.
[4] Foucault, *The Order of Things: An Archaeology of the Human Sciences*.

nominations," by which he means that language itself is nomenclature (used for naming).[5] Essential nominations are "self-defining and transparent" and, Foucault remarked, distinguished from "code" names. In fact, during the seventeenth and eighteenth centuries especially, the taxonomy is an encyclopedia, nomenclature, and dictionary all at the same time.[6] Slaughter, for instance, argues that because "classification was the episteme" the nomenclature which accompanies it "simply follows automatically."[7] The principle idea behind taxonomical languages is that categorization comes at the same time as naming, and that this form of ordering (classification) was an essential feature of taxonomic language planning.

The medieval theory of the Great Chain of Being previously provided scholars much the same function as *taxinomia*—as a framework for understanding the orderliness of creation. However, by the seventeenth century the explanatory power of the Great Chain of Being was all but gone. The intellectual vacuum caused by the fading influence of the Great Chain of Being was filled, in a rather surprising way, by the resurgence of essentialist taxonomy. Renewed interest in taxonomic thinking occurred, in part, because ongoing scientific reformations had failed to overturn particular fundamental assumptions about order and knowledge that were shared by most scholars before Newton. For all of their efforts at reformation, the new scientists maintained the view that nature is based on ordered principles, and that these ordered principles could be known and represented.[8] Aristotelian taxonomy thus conveniently fit into this assumption about universal ordering.

During this time, scientists and writers were increasingly discovering the power of cryptography. From the sixteenth century onwards, the techniques and technologies of writing were rapidly advancing, and led to, in the words of the seventeenth century priest, Jean Belot, the development of a "new rhetoric."[9] The associations of language and cryptography remained throughout the centuries. Edgar Allan Poe, for example, argued that cryptography was co-invented with writing itself, and therefore cryptography was in some sense internal to writing.[10] This view continued to appear in contemporary analyses of language and writing, as, for example, by Derrida,[11] or George Steiner, the

[5] Ibid., 67.
[6] Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*.
[7] Ibid., 69.
[8] Ibid., 4.
[9] Brann, *Trithemius and Magical Theology*, 199.
[10] Rosenheim, *The Cryptographic Imagination*, 20.
[11] Derrida, "FORS."

latter who echoed Poe with his suggestions that cryptography "is probably as ancient as human communication itself."[12]

Stephen Clucas has suggested that to modern ears it is difficult to understand the alliances that existed between cryptography and language planning, despite their essential connections.[13] Despite this difficulty of interpretation and relative lack of scholarly attention, this chapter seeks to identify the pathways that are essential to understanding this particular intellectual climate, when cryptography was a vitally important ingredient to many of the artificial language schemes seeking philosophical, universal, and perfect representation and communication.

4.1 LANGUAGE PLANNING AND MODERNITY

Outside of the occasional reference to Esperanto, language planning is rarely a topic of discussion today. Yet, language planning was *the* scientific pursuit of the seventeenth and eighteenth centuries.[14] Although few scientists spend much time thinking about scientific representation and communication today (save, perhaps, work on chemical notation, plant and animal taxonomy, and some other important but minor activities), in the seventeenth and eighteenth centuries, scientific method, representation, and communication were inextricably linked. Artificial languages were a critical fulcrum upon which science turned. And as such, planning an artificial language to work as a truly universal medium had an enormously important role in scholarly conceptions of modernity. Although some language planners were less "modern" than they themselves might have hoped, the projects were, almost without fail, seen as a break from prior epistemic and communication activities. Modernity and language planning were inextricably tied, as historians of the last few decades have noted many times.[15]

---

[12] Steiner, *After Babel*, 175.

[13] Clucas points to Henry Percy's 1594 work that combines early forms of cryptography with symbolic characters and various forms of notation; Rossi, *Logic and the Art of Memory*, vii.

[14] There are really two, somewhat separate, language reformation efforts occurring throughout modernity, the earlier artificial language planning movement inaugurated by Bacon and later becoming a critical activity of the Royal Society in the seventeenth century, and the Port Royal "universal grammar" plan discussed at length by Foucault in *The Order of Things: An Archaeology of the Human Sciences*. The prior, under discussion here, has many connections to cryptography, while the latter (as far as I am aware) does not. Furthermore, Formigari suggests that there is very little historical influence between the two language planning traditions; see Formigari, *Language and Experience in 17th-Century British Philosophy*.

[15] A listing of all recent works on language planning would be too numerous to introduce here. This chapter's bibliography lists the dozen or so most influential works.

One reason for interest in artificial languages was that in the seventeenth and eighteenth centuries, scholars were looking beyond Latin for a suitable scholarly language, which had started to appear deficient for use with the new sciences. There are many reasons why Latin waned.[16] First, scientists sought universal and seamless scientific communication that Latin was never able to offer. Second, at the same time that Latin waned, overall literacy in vernaculars was growing. As literacy in vernaculars was growing, the market for printed books expanded into a readership not well acquainted with Latin, causing barriers to basic literacy and comprehension. Third, with vernaculars on the rise, changing literary education led to a distrust of the excessive reliance on eloquence and rhetoric linked to Latin (often associated with Scholasticism's investigation of words and not things). Fourth, and finally, Latin was the language of the Catholic Church, and so in post-Reformation England (where much language planning took hold), Latin was guilty by association. Worse still, criticisms spilled over from Latin, and caused a general attitude of distrust for *all* natural languages.

Another factor contributing to the rise of interest in language planning was the cultural outlook that many scholars held at the time, who were increasingly universal, equanimous, and pansophic in their beliefs. Scholars often envisioned cooperation among nations based on a shared language, especially as an antidote to religious strife.[17] This was an especial concern for John Amos Comenius, who, for example, like many other Continental language planners, had to face turbulent political and religious factions.[18] The influence of Comenius' interest and concern was far reaching; he used his large scholarly network to motivate many other scholars to investigate artificial languages, with the hope of utopia and nostalgia for imagined international Christendom.[19]

---

[16] See Maat, *Philosophical Languages in the Seventeenth Century*, 11. While it is obviously true that Latin did eventually die off, it is important to note that this argument has been oversold in the past, and that more recent research on language planning suggest that the decline of Latin was only one of many factors generating interest in artificial languages.

[17] Rossi and Knowlson similarly suggest that there were religious motivations for the development of universal languages; Rossi, *Logic and the Art of Memory*; Knowlson, *Universal Language Schemes in England and France 1600–1800*.

[18] See Greengrass, Leslie, and Raylor, *Samuel Hartlib and Universal Reformation*, but note that Maat, *Philosophical Languages in the Seventeenth Century* argues that the influence of Reformation politics is at risk of being overstated in secondary literature.

[19] Maat, *Philosophical Languages in the Seventeenth Century*, 9. Comenius' pansophic interests often interacted with hermetic views, however, Maat argues directly against the view held by Rossi and others that universal language schemes were influenced by mystical writers, such as Dee and Boehme. These hermetic views attributed a "signature" to things that aligned with philosophical naming schemes, used for deciphering a "divine alphabet." See chapter three for a discussion of signatures and hidden resemblances. See also Markley, *Fallen Languages* and Bono, *The Word of God and the Languages of Man* for further discussion of hermetic influences.

Similarly, Athanasius Kircher used his language scheme to attempt to renew contact with the divine, as a strategy for the religious unification of people. One can imagine that as the West made contact with new and different cultures, the world was also seen as shrinking, but without universal methods for communication, clashes would inevitably arise, therefore, demanding a suitable artificial language.

In science, taxonomic and encyclopedic approaches were growing in popularity, which was also reflected in the development of artificial language schemes. Language planners believed that language ought to map neatly on to the branches of nature. For example, Bacon was very interested in artificial languages for their role in his proposed scientific reformation. Bacon's distrust of natural language stemmed from its inadequacies for scientific communication, and its inability to properly represent nature. A well designed artificial language, it was believed, would solve issues of scientific communication and representation.

Most contemporary scholars of the history of artificial languages, however, offer little more than passing reference to cryptography. Of the works available in English that deal with the language planners, as far as I am aware, only Umberto Eco's *The Search for the Perfect Language,* Wayne Shumaker's *Renaissance Curiosa*, and James Knowlson's *Universal Language Schemes in England and France 1600–1800* spend more than a sentence describing the relationship to cryptography.[20] Even these works, however, do not fully investigate the ways that cryptography and artificial language planning are, in fact, co-determined.

For instance, Eco dedicates a chapter to "polygraphies" (which includes cryptography), but he does little to connect it to the theme of the rest of the book.[21] Similarly, Shumaker offers a wide-ranging analysis of Trithemius' cryptography and its influence, and in his chapter on George Dalgarno's universal language, he only rhetorically asks, did "the interest in cryptography stimulated by Trithemius between 1500 and 1518 [play]… a role in the

---

Stolzenberg also draws connections between Kircher's efforts at artificial language planning and cryptography. See Stolzenberg, *The Great Art of Knowing*.

[20] It should be noted that Strasser has written a considerable work in German about this particular nexus, however, only some of Strasser's work is available in English. His *Lingua realis, lingua universalis und lingua cryptologica* apparently discusses how cryptographers, and Trithemius in particular, used a real language (Latin) as a kind of pivot language between the cryptographic language on the one hand, and the artificial universal language on the other hand. All three languages could be expressed in combinatory, binary representation. See Strasser, *Lingua Universalis: Kryptologie Und Theorie Der Universalsprachen Im 16. Und 17. Jahrhundert*.

[21] Eco, *The Search for the Perfect Language*.

development [of universal languages?]."[22] But, between Trithemius' cryptography and Dalgarno's universal language, according to Shumaker, they share only the qualities of oddity, difficulty and rarity. Shumaker admits, "I brought them together into a book, knowing that the unity would be loose but feeling that the common strangeness of all four would justify their appearing together."[23] Finally, on the authority of Madeleine David's *Le Débat sur les écritures et l'hiéroglyphe aux XVIIe et XVIIIe siècles: Et l'application de la notion de déchiffrement aux écritures mortes*, Knowlson acknowledges that "the seventeenth-century works of universal writing [derive] from a cryptographic rather than allegorical [perhaps mimetic?] tradition," but, then after a page of discussing how cryptography can "be regarded as leading up to the earliest schemes of common writing," the influence is again explained away.[24] Knowlson even suggests that cryptography does not add much to artificial languages. If one must use a mechanism of transposition, Knowlson argues, then "non-figurative" (i.e., "conventional") signs are a practical necessity (that is, arbitrary signs must be used when creating flexible schemes of transposition). Knowlson also suggests that some of the cryptographic processes are handy, but rather "obvious" features of philosophical languages. According to Eco, Shumaker, and Knowlson, then, the conceptual advances wrought by cryptography provided the raw material for artificial language planners, but little more.[25]

I cannot hope to do justice to the rich histories of artificial language planners and their broad influences and effects here. In fact, I will scarcely be able to do more than note how Bacon inaugurated this rich tradition, and then offer some discussion of those schemes that followed in his footsteps.[26] The focus of this chapter is to start to redress the ways that discussion of cryptography has been

[22] Shumaker, *Renaissance Curiosa*, 138.
[23] Ibid., 10, 13.
[24] Knowlson, *Universal Language Schemes in England and France 1600–1800*.
[25] All three authors, nonetheless, spend some effort investigating a particular kind of co-articulation between artificial languages and cryptography, tracing linkages between artificial language and shorthand (so-called Tironian notes), which were thought to be a form of cryptography. Tironian notes, according to Salmon (and repeated by Knowlson), provided the model for universal, rather than philosophical, language planning. See Ibid.; Salmon, "The Evolution of Dalgarno's 'Ars Signorum.'" How shorthand and cryptography relate, is left unexplained.
[26] Scholars have since uncovered some predecessors to Bacon, but their influence on the subsequent tradition is questionable. Slaughter, for example, noted that in France, Jean Douet's obscure and forgotten work from 1627 was an early development of universal character that "evolved from work he had begun on codes and ciphers," but also from shorthand, Egyptian hieroglyphics, and Chinese writing. Knowlson notes that in 1531 Juan Luis Vives discussed a universal language. Eco also pointed out that Dante discussed a perfect language back in the fourteenth century.

neglected. This oversight in contemporary literature, of the ways that cryptography and artificial languages are actually connected, is disconnected from the reality of these artificial language planners, who often wrote about their language planning activities in terms of their investigations of cryptography. Drawing on the correspondences between artificial languages, code systems, and cryptography, I argue that the mediatic aspiration of artificial language schemes—as models of communication—is the lynchpin that connects its history to the development of cryptographic schemes.

4.1.1 Francis Bacon's artificial languages

The development of artificial language is necessary, Bacon wrote, because words in natural languages are potentially corrupting. Bacon called these corrupting influences the "Idols," which bring "false appearances," but are "inseparable from our nature and our condition of life."[27] In fact, Bacon believed, entire lives may be characterized by a world of real and metaphorical illusions, expressed as an uneven mirror, people chained to the walls of Plato's cave, the chaos of the bazaar, and the tricks of theatre.[28] Each of Bacon's Idols offer a kind of representational deficiency caused by, in large part, mimesis. The uneven mirror (called the "Idols of the Tribe"), is a necessary illusion, affecting all people with sense and mind, recalling Plato's clever fellow in the *Republic* "making" all the things by pointing a mirror (see chapter three). The people chained to the walls of Plato's cave (called the "Idols of the Cave"), see only a part of true reality, which on Bacon's account, results from the company one keeps, the misplaced authority of some books, or personal predilection and bias. The chaos of the bazaar (called the "Idols of the Marketplace"), results from the inherent deficiencies of natural language for communication and exchange, as seen in the melee of a multilingual bazaar. The tricks of theatre (called the "Idols of Theatre"), produce belief in false and fictitious worlds, just as Plato argued, with respect to designing the perfect city. Each of these problems pose challenges for science in general, but given the necessary association between science and language, Bacon focused on redressing the deficiencies of natural language in his proposal for an artificial language.

Bacon was also aware of natural languages that were less deficient, and therefore might be good candidates for reform, or at the very least might provide useful models for constructing completely artificial languages. Bacon

[27] Bacon, "Translation of the 'De Augmentis,'" 228 ii.
[28] Bacon, *Novum Organum Scientiarum* xli, xlii, xliii; Bacon, "Translation of the 'De Augmentis'" ii.

believed, like most other scholars of his day, that humankind originally spoke one pure language (Eco calls this the "monogenetic" theory of language).[29] In the Biblical Genesis story, humans attempted to construct a tower at Babel reaching up to the heavens. Before Babel, humans spoke one pure language, but as punishment for the act of hubris, God confounded communication (*confusio*), forcing the use of multiple, imperfect languages. For Bacon, the Genesis account was testimony to the fact that language was once pure, and therefore (in principle) could be cleansed of the "Idols of the Marketplace," and regain its ability to fully represent and reflect the natural world.[30] Some languages, such as Chinese, Hebrew, and Egyptian Hieroglyphs (newly discovered in Bacon's day), were thought to have retained some of the purity of the prelapsarian language.

Contemporaries of Bacon also sought the recovery and reformation of natural languages.[31] Guillaume Postel (1510 – 1581) argued that Hebrew was the original language, an opinion he came to from reading the cabalistic *Zohar*. Postel concluded that it would be best to reinstate Hebrew as a universal language. Conrad Gessner (1516 – 1565) took a similar but less radical view—he argued that Hebrew was the first language from which others developed, that is, the original, if not pure, language. Gessner came to this conclusion from an analysis of fifty-five different languages, of which, according to Gessner, all still retained Hebraic characteristics, "though in a corrupted state."[32] Claude Duret (1570 – 1611) published a history of the origins of language that also thought Hebrew was a suitable starting point for monogenetic language reformation. Hebrew was suitable because it never permitted itself to be polluted by other languages, according to Duret. Robert Fludd (1574 – 1637) held a literal and mimetic view of nature, believing that the Hebrew characters were engraved in the primordial matter of Creation. Similarly, as a participant of the "logomystic" tradition, Jacob Boehme (1575 – 1624) saw a correspondence between Hebrew characters and (magical) astrological signs. And finally, although it was somewhat less popular than Hebrew, Chinese was also sometimes associated with language reformation efforts. John Webb (1611 – 1672) thought that the Chinese language existed in a pure, pre-Babelian state (as did Bacon), since the Chinese did not

[29] Eco, *The Search for the Perfect Language*.
[30] See Bono, *The Word of God and the Languages of Man*; DeCook, "Francis Bacon's 'Jewish Dreams.'"
[31] Eco and Formigari offer extensive discussions and examples; Eco, *The Search for the Perfect Language*; Formigari, *Language and Experience in 17th-Century British Philosophy*.
[32] Gessner, quoted in Eco, *The Search for the Perfect Language*.

participate in the construction of the Tower of Babel, and therefore, their language was immune to the *confusio*.

Some scholars also developed special cryptographic tools as a means to study the monogenetic origins of language. Antoine Court de Gébelin (1725 – 1784) worried that if there were as many root words (or "radicals") as there are things in the world, then understanding the combinatory complexity of language could only be accomplished through a set of deciphering keys. Of course, the field of cryptography was already established as an effective tool for dealing with massive sets of symbols, so the possibility of using it for the scientific investigation of natural languages was a fairly obvious step. Like Bacon, Court de Gébelin thought that cryptographic schemes were are able to signify anything by any two differences (discussed below).[33] Binomial differences in nature had long been identified through taxonomic tree structures (Linnaeus was a contemporary of Court de Gébelin, although taxonomic tree structures were in use prior to Linnaeus). To better understand how differences in symbols could signify,[34] Court de Gébelin studied the etymologies of Greek, Latin, and French, as well as the icons and emblems of the world's linguistic history, and concluded that the alphabet in itself was, as Eco put it, "nothing but the primitive hieroglyphic script reduced to a small set of radical characters or 'keys.'"[35] Therefore, the origins of language were not the result of mere chance or convention, according to Court de Gébelin, but clear evidence of some underlying linguistic unity and purity that mapped on to the world.

As will be discussed further below, John Wilkins and Athanasius Kircher also used cryptological methods to assess the range of natural, potentially pure, languages when designing an artificial language. The latter developed cryptographic techniques, even material tools, to explore original languages.[36]

Hebrew, Chinese, and Egyptian Hieroglyph languages were popular topics of exploration, eventually becoming tropes of the emerging monogenesis tradition, but Bacon had further reasons to single out these particular languages. First, it has been argued that Bacon sought Jewish religious utopia, as outlined in *New Atlantis* (1627), as an integral part of scientific and linguistic utopia.[37] This fact

[33] Ibid., 94 ff.
[34] By focusing on *differences* for linguistic signification, Court de Gébelin anticipates Ferdinand de Saussure in the nineteenth century.
[35] Eco, *The Search for the Perfect Language*, 94.
[36] A fuller study of Kircher's place in the development of cryptography (with particular attention to his understanding of the language planning traditions) can be found in Stolzenberg, *The Great Art of Knowing*; Strasser, "The Noblest Cryptologist."
[37] DeCook, "Francis Bacon's 'Jewish Dreams.'"

helps explain why Bacon insisted on the originary powers of Hebrew. Second, knowledge of China was rapidly expanding in Bacon's day, and catching the interest of Western scholars. Just two years prior to the publication of the *Advancement of Learning,* a delegation of 250 men had returned from China,[38] and the West begun work on Chinese histories (often occupied by influential tales of magic and the supernatural).[39] In particular, the 1604 translation of José de Acosta's *Historia Natural y Moral de las Indias* is believed to have been a direct source of Bacon's views of the Chinese language.[40] Third, prior to the discovery of the Rosetta stone, Egyptian Hieroglyphs were poorly understood, and usually associated with an advanced and educated civilization, which, Bacon thought, ought to provide a model for social and scientific practice.

Bacon believed that the reformation of original languages, or the creation of new languages, was a necessary part of the reformation of scientific practice.[41] Scientific practice had to be reformed, according to Bacon, because the old model of a fecund Mother Nature was false.[42] Instead, Nature would only offer her secrets when forced—even tortured, with "bonds and handcuffs"—or wrestled against her gods.[43] According to Bacon, scientific investigation is a mutual struggle between scientist and Nature, with each testing the other. Therefore, if a true scientific language were to be built, it would need to be deeper and more expressive than natural and original languages alone, and integral to this stuggle. Without such a language, there would be no hope for representing Nature's complexities to the human mind.

---

[38] Lux, "'Characters Reall.'"

[39] This period of transmission also provides the backdrop to Derrida's accusations of the ethnocentrism implicit in logocentric thought. Derrida reads David's *Le Debat sur les ecritures et l'hieroglyphe aux xvii et xviii siecles* as an admission that European fascination with Chinese language is a kind of "speculative prejudice and ideological presumption;" Derrida, *Of Grammatology*, 75.

[40] Knowlson, *Universal Language Schemes in England and France 1600-1800*; Lux, "'Characters Reall.'"

[41] Slaughter suggests that Bacon saw this problem as co-articulating, or "vice versa," and Bono thought they were the "same project;" Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*; Bono, *The Word of God and the Languages of Man*.

[42] Pesic, *Labyrinth*, 24.

[43] It should be noted that Pesic's interpretation is controversial. Other commentators see Bacon's scientific practice arising from his interest in practical and mechanical arts; see Merchant, "'The Violence of Impediments.'" There is also a much larger body of literature devoted to the interpretation of Bacon's "torture" of Nature as being fundamentally gendered. This tradition does not see Bacon "wrestling" with Proteus, but rather his rape of Mother Nature. A good assessment of this body of literature is provided by Vickers, "Francis Bacon, Feminist Historiography, and the Dominion of Nature."

Even if words follow in the footprints of reason, the new science demanded a more rigorous approach. The scientist, Bacon thought, must approach nature as an examining lawyer and judge. Nature is like an obdurate witness that only reveals truth upon "vexation" and interrogation, because the "genuine forms… lie deep and [are] hard to find."[44] Famously, Leibniz later summarized Bacon's method as "the art of inquiry into nature itself and of putting it on the rack."[45] In fact, Bacon's specific scientific method ends up looking like the methods used for breaking cryptographic codes.

With Nature on the rack, Bacon's scientific method revealed secrets. But, since "particulars" result from scientific investigation, an interpretation of enigmatic results was still required.[46] For Bacon, scientific investigation places importance on particulars over universals (in opposition to Aristotelian epistemology). However, Bacon realized that by focusing on particulars, science would have to contend with their ambiguous status, as both symbol and fact. Particulars are both symbol and fact because, by themselves, they require interpretation—as symbol—yet stand alone, as bare and particular facts of nature. As discussed in chapter three, in the age of resemblances, it was thought that nature required interpretation to expose and interrogate occult properties and relationships, which were present as hidden resemblances. Bacon resisted the analysis of hidden resemblances, however, and developed his own way to interpret enigmatic particulars.[47]

Bacon's scientific method drew parallels from the "two books" tradition. According to this view, reality is expressed in the (Christian) Book of Scripture and the Book of Nature.[48] This view assumed that just as one must interpret the signs and symbols in the Book of Scripture, one must also interpret the signs

---

[44] Pesic, *Labyrinth*, 22.

[45] Quoted in Pesic, "François Viète, Father of Modern Cryptanalysis - Two New Manuscripts." There is more to the violent imagery than just good scientific practice going on here. Apparently, Bacon never used the phrase Leibniz supplied, but the sentiment is present nonetheless. In fact, at the time, it was common to identify Nature with women, often as "Mother Nature." As such, the violence of science and technology frequently takes on a gendered quality. For example, in *Judicium Jovis*, a Latin dialogue by the German Humanist Paulus Niavis, Mother Nature is pictured as brutally cut up and full of holes (from Man's mining), the very personification of rape. Bacon's scientific method is similar—in an unpublished work he speaks of Nature as a captured queen that needs to be united in "legal wedlock… with things themselves." See Pesic, *Labyrinth*, 27.

[46] Pesic, *Labyrinth*.

[47] Bacon's method had recognized limitations. Actual miracles had to be accommodated within his epistemological framework, so, his scientific method was limited on theological grounds. See Daston, "Marvelous Facts and Miraculous Evidence in Early Modern Europe," 87–90.

[48] See also Bono, *The Word of God and the Languages of Man*; Markley, *Fallen Languages*.

and symbols of the Book of Nature. Therefore, the natural scientist must be trained to read these symbols, which reveal themselves in the signs of nature. In fact, this interpretive method was not exclusive to Baconian science. Reading signs and symbols from the Book of Nature was also familiar to the Paracelsusians, occultists, and hermeticists. The Baconian and occultist approaches to symbol interpretation—as either from the Bible or Nature—were, in fact, cryptanalytic.

In his *The Clue to the Maze,* Bacon calls on science to breach the innermost sanctuary of science through interpretation using a "key" called "induction."[49] The method was thought to be inductive because the chain of permutations steps from one symbol to another, replacing combinatory relationships for logical ones. In this work, Bacon portrays himself as a new Theseus, saving humanity from the Minotaur by following a guiding thread, just as scientific method must follow a thread to interpret nature's secrets. Bacon's proposal for a specific method of induction uses a classical cryptanalytical table of *n*-grams. In classical cryptanalysis, the frequencies of specific bi-grams and tri-grams are often used to determine the underlying language of the enciphered text, and to see if certain pairs of letters from the original language are present in the ciphertext and can be exploited in cryptanalysis (see chapter nine for a full discussion of cryptanalysis and language). To understand nature, the scientist/code-breaker works through each *n*-gram combination of signs, which have been carefully written down in some suitable kind of notation. With notation in hand, the scientist/code-breaker works through the table of *n*-gram frequencies until some subtle underlying meaning is revealed.

Blaise de Vigenère, a French contemporary and fellow cryptographer, also developed a cryptanalytic technique to interpret nature, arguing that "all nature is merely a cipher and a secret writing."[50] Like Bacon, Vigenère read nature's notation, which for Vigenère, was found all around, for example, in the positions of stars in the sky or musical scores. Like Bacon, Vigenère believed that although the signs of nature were plainly visible with one's eyes, understanding such signs was difficult. To deal with this issue of interpretation, Vigenère also developed a method of transforming nature's notation, in order to make it comprehensible. Vigenère's method required that the signs could be interpreted with the aid of Jewish cabbala, which he understood as an ancient form of codebreaking that worked through permutation. In cabbala, the numbers and letters of the world cannot be interpreted directly, instead, they

[49] Pesic, *Labyrinth*, 69.
[50] Quoted in Ibid., 62.

require specific methods of transposition in order to make sense of nature's riddle. In the atbash method, for example, the technique simply reverses the alphabet; for the gematria technique, on the other hand, numerological significance is assigned to the notation, enabling a kind of divine calculus. Vigenère applied these lessons of permutation as a kind of cryptanalysis of nature, and, like Bacon, used the method for scientific purposes.

Above, I described the way Bacon interrogated nature's complexities by extracting implicit grammars from nature (which were hidden in ambiguous particulars). According to Pesic, to accomplish this interrogation, Bacon used methods of combination and analysis drawn from cryptanalytical techniques. These methods were focused on epistemic inputs, but, as I discuss below, Bacon's scientific reform also included outputs—ways to accurately and fulsomely represent nature through scientific nomenclature. In Bacon's day, it was common for scientists to use Aristotelian scientific taxonomy to represent nature. Bacon, on the other hand, developed a new method for representing nature, built from his study of natural (often original) languages. As I explain below, this programme of research led Bacon to develop a system of "Real Characters," which were notations that represented nature "directly." Real Characters developed as a system of "differences" capable of representing precisely and unambiguously. I argue that the model for Bacon's Real Characters was his notational cipher system, developed previously in his youth.

4.1.1.1 Real Characters

Real Characters are an artificial system of language that are supposed to work like numerals in mathematics. That is, for example, the inscription <2> does not refer the words two, *deux, duo*, and so on, but to a quantity itself.[51] Each Character "expresses" or represents "things and notions" directly.[52] That is, these Characters *index* things directly (like Alberti's cryptographic transformation <A> → <G>, discussed in chapter three). Departing from the opinion of his predecessors, who thought that finding rational etymologies was the central task of purifying and improving language, Bacon believed that his central task was to develop a system of grammar for indexical characters. The system of grammar comprised of Real Characters was Bacon's version of Aristotelian taxonomy, which, however, would ensure a direct connection between words and things.

In *The Advancement of Learning* and *De Augmentis Scientarum*, Bacon proposed the development of a system of grammar that worked as a "kind of

[51] Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*, 2.
[52] Bacon, "The Advancement of Learning," 230.

analogy between words and reason."[53] Bacon distinguished between two kinds of analogy for grammar: one "popular" (rhetorical) and one philosophical. The "popular" kind of analogy was literary or rhetorical analogy, which only "laid down precepts for a chaste and perfect style."[54] Bacon dismissed the "popular" kind of analogy, believing it unsuitable for development. The philosophical kind of analogy, on the other hand, was "very worthy" of development. According to Bacon, philosophical analogy is a kind of logical or mathematical relationship within a system of grammar that permits the "word" to refer precisely to one and only one "thing."[55] The analogy between words and reason is possible because the "power and nature of words… are the footsteps and prints of reason."[56] Bacon, therefore, sought to explore philosophical analogy within a system of grammar because it was guided by reason.

Even though Real Characters are philosophically analogous to things ("particulars"), they do not need to share any material or essentially taxonomic characteristics with the signified. Bacon argued that the system of Real Characters should have no "similitude" of the "thing signified," that is, he writes, they "have nothing emblematic in them."[57] In other words, the system of Characters works arbitrarily ("*ad placitum*") and is "silently agreed on by custom,"[58] having no vocal or visual similarity. Bacon concludes that the analogous relationship between the Character and the signified is indexical but by fiat, in the same way that money, Bacon points out, may be made out of materials other than gold and silver.[59] Real Characters work like money, but, Bacon argues, things and *natural* words do not essentially correspond, and are thus inappropriate for science.[60]

Pragmatically, the difficulty with natural and original languages—even if "pure"—is that natural languages are spoken, and therefore, any isomorphism between written and spoken words requires as many Characters as there are

---

[53] Ibid., 232.
[54] Bacon, "Translation of the 'De Augmentis,'" 111.
[55] Ibid., 112.
[56] Bacon, "The Advancement of Learning," 232.
[57] Bacon, "Translation of the 'De Augmentis,'" 110. We can also see a linkage here with Bacon's "Idols of the Marketplace," as well as a general dismissal of mimetic forms of representation.
[58] Ibid. See also Maat, *Philosophical Languages in the Seventeenth Century*, 18.
[59] Bacon, "Translation of the 'De Augmentis,'" 110. Bacon's belief that Real Characters must be conventional was not a view shared by all of his contemporaries and followers. The distinction between natural and conventional semiosis was not kept separate from the general problem of the origin of language. For and extended discussion, see Formigari, *Language and Experience in 17th-Century British Philosophy*.
[60] See also Lux, "'Characters Reall.'"

"radical words" (or linguistic roots).[61] This is an issue for Chinese people, Bacon erroneously thought, because they speak different languages but write in the same script.[62] So, Chinese must have a massive number of written symbols for each spoken word. But, Real Characters are supposed to index things directly. Since there are in fact a great number of things, the number of Real Characters would have to be massive, like Chinese. Bacon proposes a solution to this problem: written words can be organized logically, and therefore managed with ease. Spoken words, however, cannot be organized in the same way, so Bacon's proposal only works for written words. Real Characters, therefore, are fundamentally a system of written expression (an ideographical pasigraphy), where isomorphism only occurs between the *written* mark and thing.[63]

According to Bacon, language only requires a system of marks with suitable "differences," that is, marks "divided into differences sufficiently numerous to explain the variety of notions."[64] This "difference" must be in principle "perceptible to the sense, [and act as]… a vehicle to convey the thoughts of one man to another."[65] Many systems of language have developed over time that satisfy these minimal requirements, but according to Bacon, they all suffer from representation and communication problems. An artificial language ought to include a system of differences that are conventional, yet exclude semantic ambiguity, so that words refer to single "things" located precisely in a taxonomy (of which he never developed).[66] For his system of Real Characters, the *way* "differences" are to "act as a vehicle" is critical for how precision and abstraction can come together in a productive system of scientific communication.

Therefore, Real Characters require only as many marks as there are number and kinds of "differences" in the "things and notions" of the world. Things and notions are represented directly by the system of marks, with conventional (*ad placitum*) signs. But, what do these linguistic "differences" look like, and how do they operate? Bacon is not clear about these issues when formally discussing Real Characters. However, I argue that we can find these answers in Bacon's

---

[61] Bacon, "Translation of the 'De Augmentis,'" 110.
[62] Bacon writes, "any book written in characters of this kind can be read off by each nation in their own language." Ibid., 109.
[63] In chapter eleven the fact that cryptography is written, not spoken, will become vitally important to understand how cryptography functions.
[64] Bacon, "Translation of the 'De Augmentis,'" 109. Bacon's forward thinking view anticipates Saussure's view that language is a system of difference.
[65] Ibid.
[66] Unlike many artificial language planners to follow, Bacon does not spell out the taxonomical aspects of Real Characters, but it seems that he had a similar notion in mind, even if the scientific taxonomy was left implicit.

discussion of cryptography, and in his design for a bi-literal cipher, which was also system of binary differences.

4.1.1.2 Bi-literal cipher

In *The Advancement of Learning,* and the later Latin elaboration, *De Augmentis Scientiarum*, Bacon discussed forms of grammar necessary for the development of Real Characters. In both of these works, the discussion of grammar is followed by a discussion of cryptography, and the invention of a new cipher comprised of a system of differences (even though Bacon's cipher was published in *De Augmentis Scientiarum*, it was in fact designed earlier, in his youth). I argue that Bacon's system of Real Characters and his work on cryptography have many commonalities, and should be interpreted together, as comprising the totality of his artificial language system. The common properties of the schemes include being quick and easy, representationally powerful (both cryptography and Real Characters index their subjects, as either a plaintext letter or an object in the world), made of conventional signs, that are capable of representing all of nature, and composed of a system of differences.

Bacon's artificial language system—the system of Real Characters—was comprised of a set of differences, like his "bi-literal" cipher. This feature was essential to how these systems of representation and communication functioned. Bacon writes:

> *For hence we see how thoughts may be communicated at any distance of place by means of any objects perceptible either to the eye or ear, provided only that those objects be capable of two differences.*[67]

That is, cryptography enables the transmission of *thoughts* over vast distances by any suitable media, requiring only digital binary writing, a basic form of notation.[68] Bacon's scheme is, as far as I am aware, the first ever thoroughgoing description of a digital system.

Bacon argued that the common ("vulgar") orthography of natural language led its users to believe that there was a necessary connection between pronunciation and writing, which also led to the mistaken belief that natural language was appropriate for scientific activities. Linguistic and scientific reformation was needed to counter the inherent deficiencies of natural language and thus, at the end of his discussion of Real Characters, Bacon asks, "to what

[67] Bacon, "Translation of the 'De Augmentis,'" 118.
[68] This quasi-telepathic theme occurs over and over in the history of cryptography (and we will return to it in chapter seven).

purpose is this innovation [of Real Characters]?"[69] Bacon then writes, "Let us proceed then to Ciphers."[70]

Bacon's proposal for cryptography captures the essential characteristics of Real Characters, namely, that both systems are indexical, made of conventional signs, capable of representing all of nature, and composed of a system of differences. One significant difference between the systems is, however, the issue of *what* gets represented. As I described above, Bacon ultimately rejected attempts at natural language reformation (even for those languages thought to be original or pure), because, Bacon thought, natural languages represent aspects of speech (spoken words), requiring an untenably large number of marks to represent every linguistic radical, and, natural languages focus on the wrong things. Real Characters, on the other hand, represent things and notions directly, needing only as many Characters as there are essential properties of things.

Bacon lacked a taxonomic scheme to reduce the number of essential properties of things, but he did have a cipher scheme capable of representing all things with a minimum of marks. In its typical use, Bacon's "bi-literal" cipher reduces all of the letters of the alphabet to just two letters (for an alphabet less than 32, five letters of two types), enabling anything to be signified.[71] But, in fact, the two "letters" can be any mark capable of showing "two-fold" difference—just like Real Characters. And so, any two marks found in nature can also form the basis of the bi-literal cipher. Since the only form of representation more abstract and basic than binary is identity itself, Bacon argued that his bi-literal cipher could signify anything by anything ("*omnia per omnia*").[72] Additionally, the medium of communication could be whatever is most convenient or practical, such as "bells, trumpets, torches, gunshots, and the like."[73] Due to the wide variety of media possible, and the possibility for subtlety when inscribing differences, encrypted messages could also be hidden within a covering text or image, so as to not arouse suspicion.[74]

Let us look at Bacon's bi-literal cipher more closely. To create such a system, a set of marks must first be established—these are "notations"—that can be written unambiguously, which will comprise the plaintext and ciphertext. In *De Augmentis Scientiarum* (and *Of the Advancement and Proficiencie of Learning*)

[69] Bacon, "Translation of the 'De Augmentis,'" 116.
[70] Ibid.
[71] Ibid., 118–19.
[72] Ibid., 117.
[73] Ibid., 118.
[74] That is, "steganography," a term inherited by Trithemius' *Steganographia*.

Bacon uses the first two letters of the English alphabet (a, b), but any two determinate marks would do, such as numeral ("binary") writing (0, 1). For each figure in the plaintext (usually written words, but Bacon stresses that this could be "anything"),[75] the binary alphabet is ordered in a particular way, to create a unique series of ciphertext marks capable of representing the plaintext. For an English plaintext alphabet, and a binary ciphertext alphabet, Bacon used the minimum number of characters for the ciphertext, which are combinations of five binary characters. The number of binary marks required to represent the plaintext alphabet is determined by the combinatory "space" of the marks; if the ciphertext alphabet were comprised of more marks, the number of repetitions needed would be fewer (the mathematics of the combinatorial are 2^5 for a bi-literal alphabet representing at least 24 English letters, or a minimum of 3^3 in a tri-literal alphabet, and so on). So, for example, Bacon signifies the English letter "A" with "aaaaa", and "B" with "aaaab" (see Figure 4.1 for Bacon's complete table).

[75] Even though Bacon stresses that the plaintext could be "anything," this is not strictly-speaking true. In fact, as will become clear in chapter five, many things cannot be plaintext, at least not first without translation and transformation (which often causes significant representational violence).

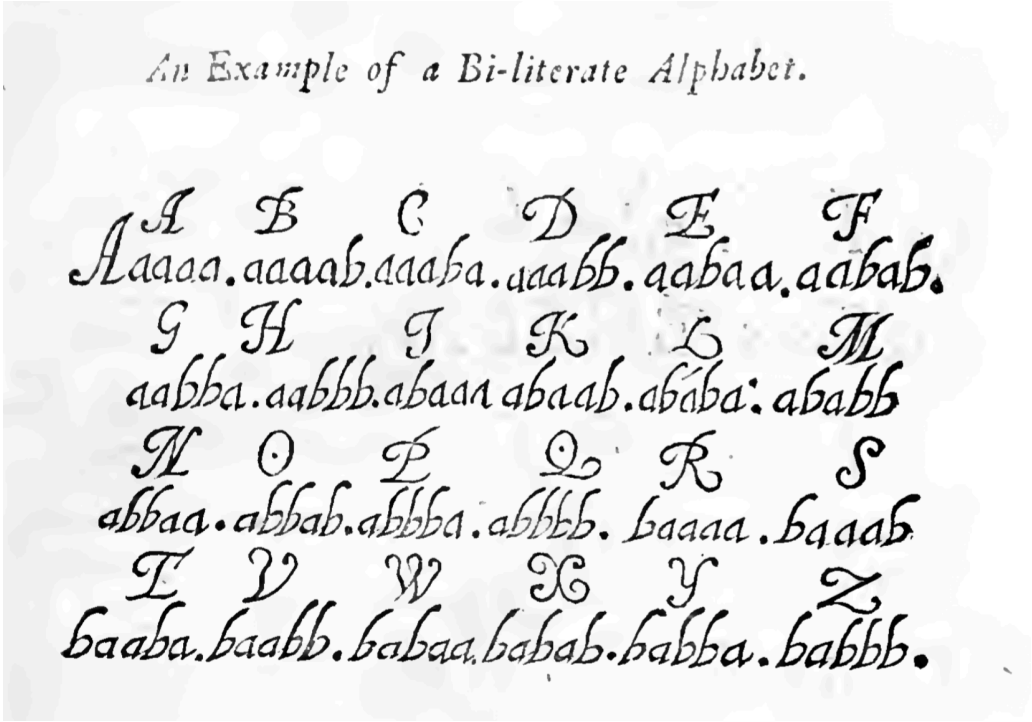


Figure 4.1: Bacon's "Bi-literate alphabet," from *Of the Advancement and Proficiencie of Learning* (1623).[76]

Thus, Bacon's cipher is a kind of notational writing that represents the world in digital terms—Nature abstracted into discrete parts ready to be transmitted across any media. The result is also a system of unambiguous scientific communication and analysis. While Bacon's desire for Real Characters was never realized (after many attempts by other universal language planners), Bacon's design for digital (artificial) writing was ultimately prescient, given the role digital writing plays in today's society.[77] Bacon's bi-literal cipher was a system of code, digital and indefinitely applicable, and capable of calculation, computation, and analysis.

4.2 THE GROWTH OF LANGUAGE PLANNING (1605–1686)

Although Bacon was not the first person to envision plans for a modern artificial language, he was its most influential advocate, and established the

[76] Bacon, *Of the Advancement and Proficiencie of Learning*, 171 book 6.
[77] Gardner offers a compelling account of the way digitality and thinking co-evolved, deriving his genealogy instead from Ramon Lull in the thirteenth century; Gardner, *Logic Machines and Diagrams*.

design for all to follow. Bacon paved the way for later scientists to use cryptographic resources for their own artificial language planning. The goal for these systems was to represent the complexity of the natural world through a tractable number of differences and their combinatorial possibilities, which was a task well suited to cryptographic processes. The alliances between cryptography and artificial languages were due to the fact that they are unified by a system of plaintext. That is, cryptography and artificial languages use notational codes which are combinable in unbounded ways, and avoid many of the ambiguities and deficiencies of natural language. Since artificial languages drew on these properties of cryptography, we might therefore consider cryptography a form of artificial language.[78] In fact, the use of cryptography for artificial language planning would be repeated by many others after Bacon.

As described in chapter three, Ramon Lull was one of the earliest influencers of the development of notational schemes, encompassing both artificial language planning and cryptography (his volvelle being a system for exploring prepositions, which later influenced the development of Alberti's cipher wheel). Both Rossi[79] and Eco[80] recognize the debt that language planners and cryptographers have to Lull. Lull sought the primary constitutive principles of all possible knowledge, and thought that logic was a (cryptographic) "key" to the hidden secrets of realty.[81] Lull's use of cabalistic combinatorial mechanisms and belief in the conventionality of language enabled a highly flexible and powerful system for combination and calculation. However, these same properties made Lull's design a touchstone for hermeticism and logomysticism (as is so common with cryptographic investigations), reaching its zenith with Rosicrucian activities in the seventeenth century, which adapted liberally from Lull.[82]

As also described in chapter three, Johannes Trithemius was an important and influential cryptographer who also developed several schemes for artificial languages, using complicated notations focused on hidden mimetic resemblances. Trithemius' systems of cryptography had many linguistic properties. According to Glidden, the cryptography outlined in Trithemius' *Steganographia* and *Polygraphia* was intended to function as a "primer" to teach

[78] I stress that this interpretation only extends to *artificial* languages, however. As I argue in chapter nine, cryptography is not a form of natural language.
[79] Rossi, *Logic and the Art of Memory*.
[80] Eco, *The Search for the Perfect Language*.
[81] Rossi, *Logic and the Art of Memory*, 29.
[82] See, e.g., Formigari, *Language and Experience in 17th-Century British Philosophy*; Shea, "Descartes and the Rosicrucian Enlightenment."

text encoding principles, and to understand the principle that "words are hidden beneath other words."[83] The tables of cryptography used by Trithemius appear, at first blush, random and magical, but in fact the columns are organized according to natural language grammars. Trithemius' work suggests a much closer connection between writing and cryptography than is usually recognized.

In language planning, many scholars followed in Bacon's footsteps, however, others came to the study independently. This included major figures, such as Descartes, Leibniz, Comenius, Hartlib, Kircher, Lodwick, Dalgarno, and Wilkins. René Descartes (1596 – 1650) had an active interest in artificial languages. Gottfried Wilhelm von Leibniz's (1646 – 1716) was also interested in artificial languages (although the fruit of this interest was never realized), and designed machines for cryptography and calculating.[84] John Amos Comenius (1592 – 1670) and Samuel Hartlib (ca. 1600 – 1662), were important because they transmitted knowledge of artificial language planning, between England and continental Europe. Athanasius Kircher's (1602–1680) work on artificial languages was considered essential reading at the time. In England, Bacon's own artificial language plans would become associated with the Royal Society. Francis Lodwick (1619–1694) was a Royal Society member and artificial language planner influenced by Bacon. George Dalgarno (ca. 1626–1687) and John Wilkins (1614 – 1672) were perhaps the most famous in this regard. Wilkins' system can be considered the high point of artificial language planning, thereafter most research activities dwindled out.

Below, I offer a brief description of this complex new era of language planning, highlighting areas of development from Bacon's designs for Real Characters and the bi-literal cipher. Central to this historical arch were the ways that Bacon's views got picked up in England and Europe, often developed alongside large and sophisticated taxonomies. The zenith of the language planning movement was clearly John Wilkins' artificial language, developed under the auspices of the Royal Academy. Although many of these language planners had proximate relationships to cryptography or quasi-cryptographic systems, Wilkins' work is notable in that it parallels Bacon's. Wilkins' artificial language system drew directly from his earlier work designing a cryptography scheme. With these histories in mind, I argue that the connections between artificial language planning and cryptography are conceptually grounded in ideas of notation and combination.

[83] Glidden, "Polygraphia and the Renaissance Sign: The Case of Trithemius."
[84] See chapter ten for a description of Leibniz's calculation and cryptography machines.

Although the details are murky, René Descartes was informed of artificial languages by one "Des Vallées," who wrote a "codebook" style universal language, corresponding with Descartes in 1629.[85] Descartes was interested in artificial languages as part of his philosophy of clear and simple ideas, but he does not seem to have developed a scheme himself. Nonetheless, Descartes was an influential advocate and communicated with numerous scholars about the matter, including Marin Mersenne and Leibniz.[86]

Leibniz hoped artificial languages would enable people to see into the "inner nature" of things like a "new telescope," and guide reason like "Ariadne's thread."[87] Like Descartes, however, Leibniz never developed an artificial language scheme of his own, but he did develop cryptographic tools. Leibniz was familiar with Wilkins' *Essay*, but expressed frustration that it was not available in a Latin version, implying that he may have not actually read it.[88] According to Cohen, the reason for Leibniz's interest for universal languages was as a "simplified notation for science."[89]

Comenius was influential to the development of artificial languages on the European continent. Approaching the topic as a pedagogue (he also wrote the first children's picture book), he believed that Latin was a difficult and deficient language, so, he supported the use of vernaculars as well as encouraged the development of artificial languages to replace Latin. Comenius believed that universal languages required universal scientific taxonomies.[90] While many of Comenius' contemporaries thought his views were indistinguishable from Bacon's (they both sought new logics of "things"), in reality, Comenius went beyond Bacon's search for keys to unlock nature. Comenius' proposed system was more than a system of writing (unlike Bacon's "Real Characters"). It was, rather, a full scientific nomenclature based on a taxonomic arrangement of primitive words and notions. Comenius believed that one must understand the classes of things, from the "outside" (empirically) and then inwards to "explore that which lieth in things, and to comprehend what each thing is in its essence."[91] Comenius's taxonomic system was an important stepping stone,

[85] Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*, 130.
[86] Ibid.
[87] Cohen, "On the Project of a Universal Character," 50.
[88] Lewis, "The Publication of John Wilkins's Essay (1668)." Lewis notes that a Latin version was eventually completed by John Ray, but it only circulated in manuscript form.
[89] Cohen, "On the Project of a Universal Character," 51.
[90] Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*, 115.
[91] Comenius, *The Great Didactic* quoted in ibid., 101.

influencing many language planners, including those in England (such as Wilkins).

Hartlib was also a key transmission figure. Hartlib sponsored many scientific activities and funded inventions, often bridging the English and Continental divide by spreading both Baconian and Comenian theories. Hartlib also corresponded with Wilkins, but it seems that their correspondence died off in the 1650s, around the same time that Wilkins moved away from hermetic traditions.[92]

John Beale was part of the Hartlib circle and developed his own artificial language. Beale's scheme was mnemonic and universal, making use of "million and millions" of "distinct" and "proper" notations. Beale's "Secret or Universall Character," was, in fact, cryptographic at its core. Beale was inspired by Della Porta's work on cryptography and specifically wanted to incorporate cryptography into his language scheme. However, despite his recognition of its importance, Beale was unable to suggest how cryptography might specifically be involved, noting only that "cryptography... hath many particular advantages."[93] Beale's artificial language would eventually make its way to the Royal Society (by introduction of Hartlib). His scheme, at seven and a half feet long and called the "grand Roll," tested the limits of combinatorial logics of his day. Beale even proposed a "further, deeper, secrete Art" that would involve ten bells rung to create "many millions" of variations.[94]

The second and third sections of Kircher's *Polygraphia nova et universalis ex combinatorial arte detecta* were devoted to code systems that were in equal parts linguistic and cryptographic. Kircher's artificial language system used two dictionaries of terms organized into 32 tables (containing the most commonly used terms, derived empirically), which was further organized into sub-lists, to make a total of 1048 terms. By looking up a word in one dictionary (locating the corresponding letter and numeral), and then finding the appropriate encoding in the other dictionary, one could encode meaning across languages (a kind of "pivot" language). Kircher also added supplementary signs to indicate tense, mood, number of verbs, and declensions. In other words, Kircher's system performed a kind of assisted translation.[95]

---

[92] Ibid., 108.
[93] Beale quoted in Lewis, "'The Best Mnemonicall Expedient,'" 129.
[94] Ibid., 121.
[95] Eco, *The Search for the Perfect Language*, 199; Wilding, "'If You Have A Secret, Either Keep It, Or Reveal It': Cryptography and Universal Language." See also chapter nine for a full discussion of the role of language translation in cryptography.

Kircher also developed several code machines, both linguistic and cryptographic. The machines were small boxes with slats that moved in and out to manipulate various written notations, creating combinatorial relationships. One of the boxes had notations explicitly intended for cryptography. Gaspar Schott, a student of Kircher's, described the box in his *Schola Steganographica* (and later in his *Organum Mathematicum*; see Figure 4.2), which appears to be a kind of transposition cipher. Kircher also developed machines for manipulating other notational systems, capable of exploring combinatorial possibilities for a range of notations. For example, the *Arca Musarithmica* was capable of producing musical scores by associating numerals with musical notation. Kircher might have first encountered the use of combinatorial musical notation, and its relation to cryptography, from Trithemius, who recommended a discrete kind of writing using musical notes in both his *Steganographia* and *Polygraphia*.[96] Through Trithemius' followers, notably Schott and Della Porta,[97] the use of musical notation for cryptographic purposes became commonplace, even by professional musicians.[98]

[96] See Shumaker, *Renaissance Curiosa*, 108, 121.
[97] Schott and Della Porta explicitly reference their debt to Trithemius, although (especially in the case of Schott) followers of Trithemius attempted to avoid the accusations of demonology that Trithemius suffered by sanitizing and critiquing aspects of his work.
[98] Tatlow, *Bach and the Riddle of the Number Alphabet*.

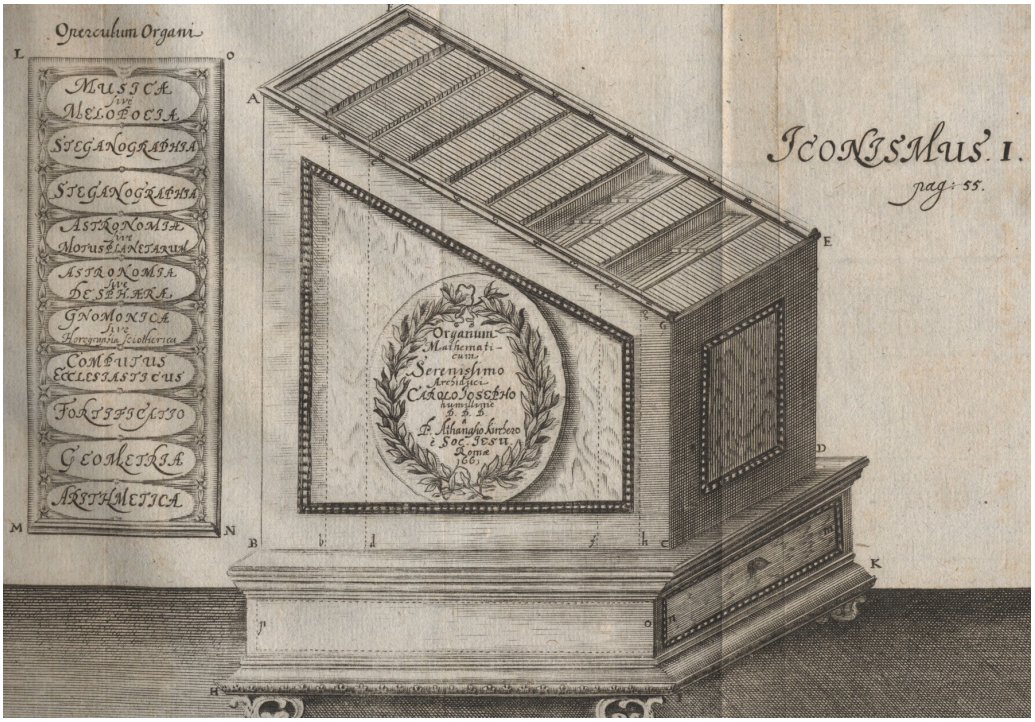


Figure 4.2: Kircher's code machine, illustrated in Gaspar Schott's *Organum Mathematicum* (1668).[99]

Notational systems for communication and memory were also common.[100] In 1626, Philip Kinder corresponded with D.P. Champagnolles regarding his writing system that used rows of numbers (presumably as symbols for words), that was "a true method for an artificial local memory."[101] Champagnolles also developed a system of communication that used pin pricks, as a kind of "digital" notation.[102] As noted previously, Trithemius also used a system of pin pricks for communication, but in his analysis of Trithemius' *Steganographia*, Schott rejects the possibility of such a method, since it attempts communication without a material medium.[103]

In 1661, Joachim Becher published an expanded version of Kircher's dictionary (which had circulated in manuscript form since 1660).[104] Becher's version contained ten times the number of items and introduced a complicated system of graphical characters representing Arabic numerals positioned along a

[99] Schott, *Organum Mathematicum*.
[100] Cf., the discussion of memory technologies in chapter three.
[101] Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*.
[102] The system was developed from 1635 but it remained secret until after his death.
[103] Shumaker, *Renaissance Curiosa*, 108.
[104] Cohen, "On the Project of a Universal Character," 53; Eco, *The Search for the Perfect Language*.

line. Soon after, Gaspar Schott published a description of Becher's scheme (*Technica curiosa*, 1664), attempting to improve upon it by simplifying the system of representation for numerals (using dots and strokes, like Champagnolles' system, which he was also familiar with).[105] Through Schott, Becher's scheme also became familiar to Leibniz (Schott also introduced fragments of Bermudo's scheme to Leibniz, which used a system of classes and corresponding numbers).[106]

Employing both Baconian and Comenian themes, John Webster published the *Academiarum examen* (1654) for pedagogical reform, with a focus on the reformation of language. Webster's proposal used ideographic characters that he thought were "Hieroglyphical, Emblematical, Symbolical and Cryptographical," and had the "wonderful and stupendous effects" of "Polygraphy, or Steganography."[107] Cryptography was, for Webster, a branch of grammar that he urged be included in classical pedagogy.[108]

Seth Ward (with the assistance from Wilkins) criticized the mystical leanings in Webster's system, arguing against the cryptographic "concealment of things," and his grammar of explication. The question facing Webster and Ward was not whether they saw a division between cryptography and grammar, but rather, whether cryptography could be considered a specialized branch of grammar.[109] For his own scheme, Ward attempted to base it on logical and mathematical principles that would connect and decompose words based on regular principles ("modal variations" or simple notions).[110] Like Bacon, Ward worried that if the number of characters needed for an artificial language was be too great, the system would be impractical. Ward's approach to reducing the number of characters was to use logic and mathematics to resolve simple notions into combinations, which then, when compounded, would be "easily known."[111]

Cave Beck was also interested in cryptography and artificial languages for use in his pedagogy (*The Universal Character, By which all nations in the world may understand one another's Conceptions, reading out of one Common writing their own Mother Tongues*, 1657). In this work, Beck envisioned a mechanical aid for speeding translation across languages, to provide "Mechanicall help for the

[105] Maat, *Philosophical Languages in the Seventeenth Century*; Eco, *The Search for the Perfect Language*, 203.
[106] Maat, *Philosophical Languages in the Seventeenth Century*.
[107] Webster, quoted in Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*, 136.
[108] Brann, *Trithemius and Magical Theology*, 223.
[109] Ibid., 231.
[110] Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*, 139.
[111] Ward, quoted in Cohen, "On the Project of a Universal Character," 154.

unlearned or such as convers with unlearned strangers," and as a "Pocket Mercury to Travaylors."[112] His design was similar to Kircher's, but it contained a semi-practical pronunciation mechanism (e.g., "cheese r 1017," or "to bore a hole 643")[113] which Kircher's design lacked.

Artificial language schemes were seriously researched by the Royal Society. Francis Lodwick was influential in later helping Wilkins with the orthography of his artificial language, and was a contributor to (and critic of) Dalgarno's schemes. Lodwick's own scheme was described in a 1657 manuscript,[114] as being "Of an universall reall caracter" which uses a notational system resembling musical notes on staff (using two dimensional positioning to indicate grammatical features).

Dalgarno published his own artificial language in 1661, titled *Ars Signorum, vulgo Character Universalis et Lingua Philosophica*. This scheme also used a combinatorial notation, which assigned a letter to each of seventeen irreducible categories, and created combinations of sub-classes within a taxonomy. However, unlike others that used binomial tree structures, Dalgarno's system developed a kind of logic within the taxonomy. For example, a symbol could stand for its opposite if amended in the right way, or could indicate other logical relationships.[115] In doing so, Dalgarno claimed to have discovered a process of "analysis logica," which was a kind of precursor to prepositional logic. Dalgarno also thought his scheme would clear up issues in grammar, logic, and metaphysics.[116] However, while Dalgarno's scheme was recognized as very useful for stenography, Culpepper, Boyle, Lodwick, and John Wallis reported that it was not practical for a universal language. Dalgarno's scheme could be spoken, however, unlike most of the other pasigraphies being developed.

The most sophisticated and famous artificial language scheme was developed by Wilkins, who in fact sketched an early version of his scheme in his cryptography manual *Mercury: or, The secret and swift messenger. Shewing, how a man may with Privacy and Speed communicate his Thoughts to a Friend at any*

---

[112] Beck, quoted in Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*, 120.
[113] See Shumaker, *Renaissance Curiosa*, 139.
[114] Knowlson reports that work on the universal language begun in 1652, and was published five years later. Note also that Lodwick published (by Hartlib) an earlier work entitled *A Common Writing: Whereby Two, Although Not Understanding One the Others Language, yet by the Helpe thereof, May Communicate Their Minds One to Another* (1647). See Knowlson, *Universal Language Schemes in England and France 1600-1800*, 74; Shumaker, *Renaissance Curiosa*, 139.
[115] Cohen, "On the Project of a Universal Character."
[116] Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*, 121.

distance (first published in 1641).[117] In this work, Wilkins considered many forms of cryptographic communication, including musical notation. Wilkins wrote, "The Utterance of these Musical Tunes may serve for the Universal Language, and the Writing of them for the Universal Character."[118] Musical notation was considered a suitable character for a Baconian universal language scheme because musical notes are discrete across time (marked by a beat, or different "Times" as Wilkins says), as well as sonically discrete (marked by "different Tones"). Therefore, it would be possible to have "each letter of the Alphabet be rendered by a single sound."[119]

Wilkins also took inspiration from Francis Godwin's work. Godwin's *Nuncius inanimatus* ("Dead Messenger") (1629)[120] described a system of communicating at a distance. In *Man in the Moone,* Godwin imagined a population of lunar people who speak in musical notes.[121] Godwin's description of musical notation for communication in *Man in the Moone* was likely the source of inspiration for Wilkins.

In *Mercury*, Wilkins also introduced code systems composed of dots, lines, and disjoint coordinate systems ("By Points, Lines, and Figures mixed together").[122] Despite looking very different from musical notation (see figure 4.3), these systems are also notational. Wilkins argued that the geometric figures he sketched for his system of plaintext representation must use non-arbitrary distances between points—each letter should "be described at equal Distances."[123] Therefore, this is a "differentiated" form of representation, which is, as will be described in chapter five, an essential feature of "proper" notation.

---

[117] *Mercury* was first published in 1641, and then again in 1694 and 1707 (in a collection of Wilkins' philosophical and mathematical work). The third edition is available in a modern printing with commentary by Brigitte Asbach-Schnitker; Wilkins, *Mercury: Or the Secret and Swift Messenger*.

[118] Ibid., 75.

[119] Ibid.

[120] Poole discusses another potential source of common interest between Godwin and Wilkins, a small (1300 words) manual for the development of an expedient character by a London schoolmaster Henry Reynolds, called "Macrolexis" (Far Reading). Reynolds had an acknowledged interest in cryptography, shorthand and telegraphy and made use of other media developments (some first discussed by cryptographer Della Porta; see Zielinksi), such as shuttered lights, fireworks, smoke signals; Poole, "Nuncius Inanimatus. Seventeenth-Century Telegraphy"; Zielinski, *Deep Time of the Media*.

[121] See Davies, "Bishop Godwin's 'Lunatique Language.'"

[122] Wilkins, *Mercury: Or the Secret and Swift Messenger*, 47.

[123] Ibid., 50.

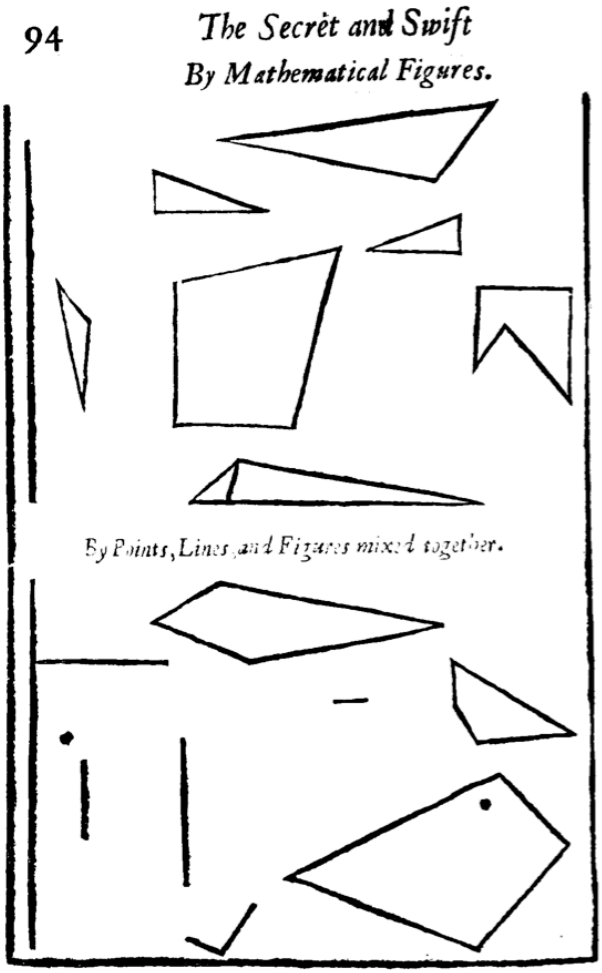


Figure 4.3: Wilkins' system of encryption by Points, Lines, and Figures.[124]

In *Mercury*, Wilkins developed a "secret and swift" form of writing capable of spanning both distance and time. Echoing Platonic themes about the influence of writing, written expression, Wilkins noted, permits "discourse with… [people] that are remote from us," simply because letter carriers are able to transport written messages in material form. The medium of writing, according to Wilkins, is effective because it does not introduce mistakes or ambiguity, and is not subject to memory loss. Similarly, Wilkins notes, writing can span the *time* "of many Ages" because, unlike speech, writing persists across time.

[124] Wilkins, *Mercury*, 94.

To develop a system of "swift and secret" communication, the particular medium needs to be able to communicate across "many Ages," or as far as to the "Moone." Such a sophisticated medium required exacting construction. In this regard, Lewis argues that Wilkins' choice of Joseph Moxon to cut the type for the *Essay* is significant.[125] According to Lewis, Moxon elevated the letterform to a position fit for notation, making "Typography... a Mathematical Science."[126] This, Lewis notes, is exactly what the *Essay* demanded, since the smallest typographical error in the printing of any character would entail a fundamental change of sense within it.[127] Despite his employment of Moxon, such exacting media requirements, however, were still beyond the technological capabilities of Wilkins' day. In addition to numerous errors (even introducing errors in Errata), Wilkins still needed to resort to hand-written additions to his complex printed notation.[128]

Finally, Hooke's unpublished fragment, "Mathematical Language," from 1686 was the last of the modern universal languages. By the end of the seventeenth century all of the original language planners had died (Hooke lasted the century, but became a recluse in the end). Shortly after Hooke's fragment, Newton's *Principia mathematica* and Locke's *Essay Concerning Human Understanding* were published, and ushered in a new kind of science. The science behind the search for artificial languages was definitively turning in the direction of logico-mathematical calculi, rather than empirical taxonomic systems. In the end, the plans for artificial languages died, but from their notational innovations, a new mathematical science flourished. Cryptography, too, lost its former association with artificial language, and increasingly became a product of mathematical thinking.

❦

The retreat of artificial language planning did not spell the end of the notational epoch. The combinatorial machines that manipulated notation became better at handling mathematical calculations—first as proto-computers and calculators, and later as actual computers—at the expense of their capabilities to function as artificial language devices. In the next chapter, we will see how these machines were capable of ordering representations of objects, because they excluded ambiguity and semantic richness—a fundamental challenge that the artificial language planners had long grappled with.

---

[125] Lewis, "The Publication of John Wilkins's Essay (1668)."
[126] Ibid.
[127] Ibid.
[128] Ellison, "Millions of Millions of Distinct Orders."

In part due to this increasing mathematization and instrumentalization, cryptography flourished—increasing in scope, power, and effect. By the end of the twentieth century, cryptography was thoroughly democratized, and responsible for mediating most global digital communications. At the same time, other media technologies—such as radio, television, and film—received considerable scholarly attention. Yet, despite the immense impact of cryptography today, beyond working cryptographers and engineers (utilizing mathematical and instrumental notions of cryptography), very little attention has been paid to how cryptography mediates communication.

5
Notation from the eighteenth to the twenty-first centuries

Western culture, wrote Friedrich Kittler, was inaugurated by encoding the Siren's song into Homer's *Odyssey.* At first, Homer and his rhapsodes transmitted the song orally. Then, the later Greeks encoded the Siren's song into technical media. They were able to do so, Kittler argued, because for the first time in history they had invented a vowelized alphabet capable of representing all sounds.[1] In *Musik und Mathematik,* Kittler literalized Odysseus' passage past the Sirens:

> *AEIOU: What is that? In your, my, our ears? A pure miracle, for the world dawns. We hear that we hear. AEIOU, invented one night.*[2]

Despite Kittler's brazen acceptance of Greek myths and the Eurocentrism it implies, the narrative is nonetheless essential to the development of notation. It is an odd quirk of history that the alphabet was invented once, and that the vowelized alphabet was invented once, and that this all happened in the West. For all of the remarkable advances of the East, the dominant language groups never possessed an alphabet, and therefore (as I describe in this chapter), they possessed different epistemic resources, unlike those needed to develop a system of notation. That notation later rose to prominence—in computing technologies, above all—is a later history, about the technological empiricism of the West and its consequent rise to power. The essential disjuncture in this narrative, however, was the invention of notation, against the presence of voice, which became recordable after the Greeks.

According to Kittler, the world dawns with the invention of AEIOU, the pure miracle of vowels. And so, the culture of the West, Kittler argued, was not invented from trade or politics, but rather by this initial rupture of writing practices—originating, from "wine, women, and song."[3] Because the founding of the West was so important for Kittler, he devised a test for Odysseus'

[1] The alphabet does not record every sound in its original way, and there are many non-Western languages that use kinds of speech that are not representable within the Greek alphabet (such as the tonal aspects of Chinese). Nonetheless, within the Greek culture, this was a significant breakthrough.
[2] Kittler, quoted in Peters, "Assessing Kittler's Music Und Mathematik," 31.
[3] Ibid., 32.

veracity, to determine whether the West was founded on a true myth. Acquiring funding from the German government, Kittler hired three sopranos from the German National Opera, whom he instructed to stand exactly where the Sirens stood two thousand years prior. Then, on his command, these sopranos sung as captain Kittler sailed alongside, just like Odysseus had two thousand years prior. The result of Kittler's experiment was to confirm that Odysseus must have lied, since Kittler could not hear the singers no matter how close he came to the water's edge. Since the tale of Odysseus was a lie, Kittler concluded, it must have meant that "Homer was setting a false trail: what he's telling us between the lines is that Odysseus disembarked, swam to the rocks and fucked the Sirens."[4]

But Odysseus' fuck was special. In fact, Western "culture" did not exist prior to Odysseus' travels. Compare Odysseus's myth with Kittler's other hero, the Egyptian King Akhneten. King Akhneten fucked his wife several hundred years prior, but he did not inaugurate Western culture. Western culture was not inaugurated for the simple fact that we don't know what he called "his N-f-r-t-t."[5] Unlike Odysseus' fuck, the Egyptians had no way to record Queen Nefertiti's screams of passion. And so, the inauguration of "Western culture" had to wait until a Greek invention: a vowelized alphabet capable of capturing and storing all human sounds (or so the Greeks believed).

To the extent that this Eurocentric narrative is true, the fact that the Egyptians lacked a suitable recording technology for screams of passion or Siren songs is not as essential as Kittler believed. The Egyptians had *notation*, which, since the beginning, had silently informed the history of reading, writing, and speech.[6] In fact, the invention of the vowelized alphabet enabled recording all speech sounds, and therefore (it was thought), all meaning could be recorded. The vowelized alphabet thus created a special relationship between Being and thought, in ways that previous writing systems did not. With their vowels, the Greeks locked voice and writing together, and so writing and speech developed together, in important, essential ways,[7] against the development of notation.

By the age of resemblance (see chapter three), with the invention of movable type presses and combinatorial machines, the combination of voice and writing

[4] "Tom McCarthy Remembers Friedrich Kittler."
[5] Kittler, quoted in Winthrop-Young, *Kittler and the Media*, 91.
[6] In fact, the Egyptian hieroglyphs were only partially notational, because they were only partially alphabetic; all alphabets are notational but not all notation is alphabetic.
[7] This is the lesson to be drawn from Derrida's work on grammatology. See Derrida, *Of Grammatology*.

that resulted from the Greek invention of the vowelized alphabet was, once again, unlocked.

The development of combinatorial methods in this era upended the primacy of voice, and therefore ruptured its association with Being and its hold on meaning. As such, the history of notation offers a counter-argument to the essential relationship between vowlized writing and the rise of the West with "wine, women, and song). As will become clear in future chapters,[8] "writing" became combinatorial ordering, which correspondingly changed "reading"—making it impossible to *speak* the written word.[9] In the age of resemblances, meaning was a product of the combinatorial relationships between written marks. Then the age of resemblance came to an end, and the voice reemerged as the origin of writing (returning to the Greek discourse network).

In this chapter I discuss the ways that from the late eighteen century forwards, the "discourse networks" of reading, writing, and mathematics shifted around cryptography and its relationship to "notation." I close this chapter with a very specific articulation of what notation is, drawn from the late American philosopher Nelson Goodman.

Specifically, this chapter covers the history of notation, after circa 1800, when the combinatorial experiments of the age of resemblance were dismissed as foolish, and the original "Greek alphabet" was reintroduced and took force in a novel way, ultimately reanimating the intimate relationship between writing and voice. Voice took on renewed importance, as oral machines replaced combinatorial machines, but programmed, this time, by the Mother's Mouth. The result, from circa 1800 to 1900, was a form of "universal alphabetization," which gripped the ways that reading and writing were developed and were used. Ultimately, however, this process of universal alphabetization was but a brief interlude. By circa 1900, Nietzsche's curse, of blindness and madness, cast a new pall on reading and writing, eternally returning to the combinatorial experiments. The Nietzschian return to combinatorial experiments, however, no longer found its grounding and origins in resemblances. That is, while the combinatorial machines of the age of resemblance grounded their existence in nature or the Real, after 1900, a new kind of technicity arose with the invention

[8] Compare with chapter nine, which focuses on the role of translation and language, and with chapter ten, which focuses on combinatorial ordering.

[9] See chapter eleven, where I argue that ciphertext cannot be spoken. One of the arguments presented in that chapter has to do with the fact that the phonemes necessary for speech are destroyed by encryption, which produces ciphertext that is typically a jumble of letters or other symbols.

of typewriters and then algorithms, grounding combinatorial reading and writing in "random generators."

Simultaneous to this history of reading and writing (there are many such histories), also starting back in the eighteenth century, the field of mathematics was developing new, sophisticated notation. Notation was being developed in order to deal with numerical calculations and more complex, and ontologically problematic, phenomena, such as infinitesimals. As language planning faded (loosening its ties to cryptography; see chapter four), from the seventeenth century onwards, the increasing sophistication of mathematics was enabling new and deeper understandings of the field of cryptography.

The mathematization of cryptography occurred in parallel to the movements in reading and writing, through the discourse networks 1800 and 1900. Then, throughout the 1900s, but especially by 2000, mathematics and reading and writing were united in new technical applications, as coded algorithms running on computers. After 2000, the machines of our daily life profoundly notational and combinatorial, as though born of cryptographic origins. The result, in actuality, and potentiality, is that from the long history of notation and plaintext, most writing became encrypted.

5.1 Discourse Network 1800

The first task of the discourse network 1800 was to eliminate the combinatory games inherited from the age of resemblance. Previously, decomposition and composition followed the rules of the combinatory system—always returning to the signifieds (to "nature").[10] The critical change that occurred in the discourse network 1800 was the switch from combinatory systems dictated by natural systems and external logics, such as Lull's volvelles or Kircher's music boxes, to meaningful, spoken articulations. Pedagogical primers were a critical site of influence, reflecting how the changeover from one combinatory technique to another occurred.[11] Within the pages of these primers, a crusade was launched against the nonsense generated by previous combinatory techniques. In fact, it became a point of honor for the authors of the primers to include only meaningful words in their works. With new importance placed on language training, this new kind of book delegated the task of educating the youth to the "Mother's Mouth."

[10] Kittler corroborates the assessment I offered in chapter four—that "the secret behind every '*characteristica universalis*' [Real Character or artificial language]" is the return to signifiers. Kittler, *Discourse Networks 1800/1900*, 44.

[11] Ibid., 45.

Pedagogical primers taught mothers to use a phonetic method when educating young men. Rather than having young men imitate adult speakers, the phonetic method enforced a "methodological exploration of the oral cavity."[12] The mouth became the new instrument for the production of meaning, which produced the belief that an alphabet (now produced in the mouth) could exist without writing.[13] The optical form of the letter—the dominant form since the invention of the printing press—was consequently subsumed by the spoken word.

The primacy of speech over writing in the discourse network 1800 was made even clearer by the introduction of machines that emulated the oral cavity. In 1780, the St. Petersburg Academy of Sciences held a competition to "instrumentally" reproduce the "all" five vowels (a, e, i, o, u).[14] Christian Gottlieb Kratzenstein entered his monograph detailing methods of vowel synthesis, and won the competition. In this work he made use of "flutes" or resonators, which were specially crafted to model the oral cavity, and based on experimental research on anatomical measurements of the human head (see figure 5.1). The pedagogical primers accomplished the same, but encouraged the exploration of the oral cavity in a more restricted way. Unlike the voice synthesis machines, the primers sanctioned the association of sounds, permitting the vocalization of only some of the possible graphical signs and combinations. That is, any combination of letters that produced sounds that were not meaningful articulations were excluded, such as the sounds of animals (that is, not humans), imbecils, or the mad.[15]

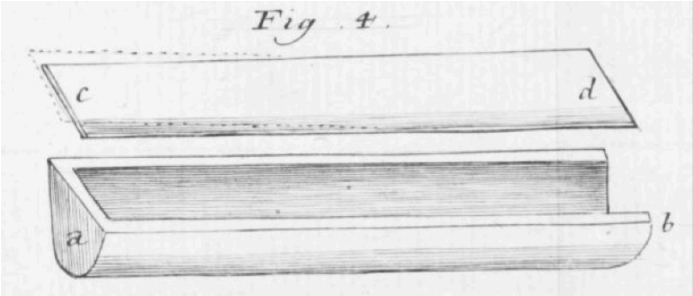


Figure 5.1: Figure 4 [vowel resonator] from *Tentamen Resolvendi Problema ab Academia Scientiarum Imperiali Petroplitana ad annum 1780 Publice Problema*.[16]

[12] This fetishization of the voice is a direct descendent of activities like von Helmont's literalization of the logomysticism of Hebrew letters (Helmont, *The Alphabet of Nature*.).
[13] Kittler, *Discourse Networks 1800/1900*, 35.
[14] Ohala, "Christian Gottlieb Kratzenstein: Pioneer in Speech Synthesis." Kittler discusses the same event, but gets some of the details incorrect.
[15] Kittler, *Discourse Networks 1800/1900*, 183.
[16] Ohala, "Christian Gottlieb Kratzenstein: Pioneer in Speech Synthesis."

Thus, at the end of the eighteenth century, the dominant aspect of the discourse network was "universal alphabetization," that is, the process of pronouncing consonants and vowels by (wooden or oral) machine and the phonetic method of reading. This process created new kinds of readers and writers, who were oriented primarily towards the voice. And so, the combinatorial method of reading and writing that had persisted from Lull to the last artificial language planners had ceased, and private, hermeneutical reading had taken its place. With the techniques of universal alphabetization, the production of meaning became a result of the relationship between written and spoken words (whereas previously, meaning was found in the resemblances between things, often in hidden or occult ways). The result of this shift was that, by 1800, spoken words then appeared "present" and meaningful to the reader—literally inside the body—no longer arranged, calculated, or enciphered by a combinatory machine.

Derrida pathologized this network of universal alphabetization. In his *Grammatology*, Derrida wrote a long history of the voice, which culminated with Rousseau as a transitional figure in the eighteenth century. According to Derrida, speech and writing are different but ultimately locked in a symbiotic relationship we call language. We can describe our knowledge of writing and speech but we cannot break out of the union, at least not from within language itself. Derrida approached this union by arguing, infamously, that there is "no outside-text" ("il n'y a pas de hors-texte").[17] In doing so, Derrida questioned this founding moment of Western culture, the philosophical belief[18] that speech is "present." When Plato and Aristotle subjugated writing to speech, the infinity of differences, delays, and gaps actually existing were covered up with a belief that a stable, self-identical present emerges. Derrida called this philosophical position "logocentrism," the view that speech is the ground or essence of this "presencing," that is, a prioritization of *phone* over *gramme* (what Kittler called the optical and acoustical division of reading and speaking). Therefore, Derrida concluded, there is no "outside-text" simply because speech and writing are symbiotically related.

The differences and gaps in language that Derrida identified are acts of violence, much like the violence implied in the gap between natural language and plaintext. Each system of expression brings about its own identity, and to

[17] Derrida, *Of Grammatology*. Since this quotation is so consistently misinterpreted, I'll note that this does *not* mean that Derrida believes, as is sometimes supposed, that "everything" is text. A good description of the correct way to interpret Derrida's claim is found in Bradley, *Derrida's Of Grammatology: An Edinburgh Philosophical Guide*.

[18] According to Derrida, philosophy *itself* is a symptom of this event.

impose one on another is to erase how and what that expression relates, represents, or describes. This violence is everywhere, and necessary, but also, the violence is sometimes overdetermined. We might consider how the alphabet amounts to, in essence, a way to impose on speech. Rather than actually describing a (supposed) deeper phonetic reality, the alphabet offered language a readily available model of how the problem of representation might be tackled.[19]

5.2 Discourse Network 1900

The discourse network of 1900 began with a curse. Half blind and half mad, Nietzsche cursed the "universal alphabetization" of 1800. It was a lie, Nietzsche thought, because readers only guessed at meaning by reading a couple of words in each work—and readers thumbed through many hundreds of books, becoming bookworms. For Nietzsche the philologist of 1800, thumbing through so many books, was no longer a possibility on account of blindness, and so Nietzsche stopped reading books and began to experiment with a telegraphic writing style.[20]

The hermeneutical reading of 1800 was also the beginning of self-deception. That is, guessing at meaning meant the reader could interpret a written work in any way she thought appropriate, deceiving herself into believing she was free to do so. The act of hermeneutical interpretation, thus, turned the reader into the writer (believing that new meaning could result in the act of reading), a shameful act of the reader's hubris, according to Nietzsche.

Liberated from this tendency for interpretation on account of his blindness, Nietzsche replaced handwriting (which requires visual inspection of the writing hand) with the Malling-Hansen typewriter, originally designed for the blind.[21] This change in technology meant that the continuous nature of handwriting was replaced with the staccato rhythm of the typewriter. And the continuity of handwritten words no longer reflected the "continuous transition from nature to culture."[22] The wellspring of writing became "selection" from a "countable, spatialized supply," as keys on the typewriter substituted for natural investigation.[23] Thus, the typewriter removed the mimetic "image of the word"

[19] Harris, *The Origin of Writing*, 38.
[20] Kittler, *Discourse Networks 1800/1900*, 193.
[21] Ibid., 191.
[22] Ibid., 193.
[23] Ibid.

(in handwriting), and replaced it with the "spatial arrangement of the letter keys."[24]

And so, with no more interpretation, and writing occurring telegraphically through a typewriter, in 1900 language becomes a medium among others. As a medium, language translation no longer exists (as a positivity for the discourse network), and the "only tasks" remaining for the keyboard are transposition.[25] Like a transposition cipher, permutation and combination were the countable measurements of the typewriter's total ability. Writing, therefore, was grounded in a (cryptographic) "random generator,"[26] which played out like a dice game.[27]

Although we usually only think of the typewriter in terms derivatively reflecting the spoken word, or the hand-written manuscript, the typewriter is actually more cryptographic than the combinatorial machines from the age of resemblance. Before the typewriter, scientific writing followed the logics of combinatorial machines investigating Nature. The invention of the typewriter meant writing was, for the first time, according to Kittler, "entirely based on randomness and combinatorics,"[28] and now unshackled from reflecting nature, it was also purified of mimetic influences. In fact, with its set of distinct keys, the typewriter is only a set of "differences," reminiscent of Bacon's bi-literal cipher (discussed in chapter four) and therefore grounded in combinatory entropy.

Writing circa 1900, Saussure described a growing notational attitude, and made a distinction between "necessary and arbitrary, graphematic and graphic differences between letters."[29] Saussure described writing as:

> *The same person can write t for instance, in different ways.… The only requirement is that the sign for t is not to be confused in his [or her] script with the signs used for l, d, etc.*[30]

Describing writing as a set of differences is precisely the establishment of notation. And so, from 1900 onwards, language effectively becomes plaintext, as notation, a technical medium.

---

[24] Ibid.
[25] Ibid. See chapter nine for a discussion of translation, and how it is distinct from cryptography. This consequence can be seen in either a positive or negative light. With only the processes of transcription remaining as tasks of the discourse network 1900, transcription becomes like a universal language (as discussed in chapter four). On the other hand, with translation ceasing to be a task for the discourse network 1900, those translators labouring away in that era did so under the false pretense of being essential to the era.
[26] Ibid., 187.
[27] Ibid., 213.
[28] Ibid., 210.
[29] Ibid., 254.
[30] Ibid.

The discourse networks of 1800 and 1900 identified by Kittler, however, are not the complete story of writing. Once a colleague of Kittler's, Wolfgang Ernst also investigated the shifts of technical media throughout the same period. Ernst notes that in the landscape of an eighteenth-century engraving of a cathedral (which "the book" was supposed to kill), stood a semaphore device (presumably Chappe's optical semaphore system). This insight demonstrated, according to Ernst, that writing was not only prefigured by the invention of the printing press and the mass production of books, but by telegraphs that were a form of "signal processing [that] will replace discourse and cultural semiotics."[31] And so, according to Ernst, the rise of technical media displaced the "traditional [mimetic] visual rhetoric of representations."[32]

Moreover, throughout this period cryptography was actively developed, and was a critical informant to the transformation of writing (a fact evident by the cryptographic logics of permutation and combination, discrete symbols, difference, and grounding in "random generators"). As well, notation continued to be developed within the mathematical sciences, leading to "computation" and machines that made fast and complex calculation possible.

5.3 NOTATION AND MATHEMATICAL SCIENCES

With the onset of mathematical sciences at the end of the eighteenth century, corresponding to the brief cessation of the notational function within writing, notation instead took on renewed importance in the emerging sciences. Developing the correct notation for representing mathematical laws of nature was an important Enlightenment activity, and by the nineteenth century, calculating machines manipulating the laws of logic and mathematics were becoming common. Mathematical notation, from Leibniz to Boole to Hollerith, contributed to computing and information systems in important and still largely unexplored ways.[33]

Mathematical notation was once considered a special kind of writing. Since the very first scripts, writing down numeric values was an important part of commerce, but extant notation was generally regarded as ponderous for

[31] Ernst, *Digital Memory and the Archive*, 39.
[32] Ibid., 40.
[33] See also Iverson, "Notation As a Tool of Thought." Iverson discusses how mathematical notation must be universal and unambiguous. Iverson thinks computer programming languages are deficient in some ways to mathematical notation, but in the best cases they "offer important advantages as tools of thought," because, unlike mathematical notation (at least prior to Wolfram's *Mathematica*), they are executable.

calculations beyond simple arithmetic. For instance, a great deal of Babylonian cuneiform contains mathematical notation, but because the notation required the same number of marks as there were things, its use was limited. The Greeks developed a numeric notation (perhaps following a model by the Phoenicians, as they did with the invention of the vowelized alphabet) that was able to represent multiple things with a single mark.[34] After the Greeks, mathematical notation continued to develop, but slowly. Roman numeral notation made it slow and difficult to perform mathematical calculations, and invited error. Even by the Renaissance, mathematical notation was still a barrier to science and commerce (recall Alberti's complaint that scribes could not accurately copy numerals, prompting him to provide explicit instructions about writing out numeric values in longhand). Wolfram summarizes the intersection of mathematical and other writing schemes:

> *[E]ven though math notation hadn't gotten going very well by their time, the kind of symbolic notation used in alchemy, astrology, and music pretty much had been developed. So, for example, Kepler ended up using what looks like modern musical notation to explain his "music of the spheres" for ratios of planetary orbits in the early 1600s.*[35]

At the end of the seventeenth century, mathematical notation was on the cusp of a breakthrough. The earlier experiments with sophisticated new kinds of notation for artificial language planning and cryptography had advanced the field considerably.[36] In fact, mathematical notation that had once been a barrier to progress became a driving force. Wolfram notes that Newton wrote the *Principia* with very little notation (apparently "Newton was not a great notation enthusiast"). Leibniz, on the other hand, made considerable use of notation, believing that the right notation was the secret to many human affairs.[37] Indeed, while still a young man writing his *Dissertatio,* Leibniz experimented with new kinds of notation for representing combinatorial mathematics (adapted from Mersenne).[38] Later, Leibniz also came to believe that the right notation for artificial language schemes was essential, but never developed one himself. One of Leibniz's most successful and lasting contributions, in fact, was his notation for infinitesimal calculus. Understanding infinitesimals was a major challenge to the field of mathematics, and developing the correct notation—clear, tractable,

[34] Wolfram, "Mathematical Notation: Past and Future."
[35] Ibid.
[36] See chapter four.
[37] Wolfram, "Mathematical Notation: Past and Future."
[38] See chapter four for a description of Leibniz's combinatorial notation.

and efficient—played a significant role in its overall acceptance. Newton's dot notation was a roadblock to calculating, and it took some time for Leibniz's notation to be accepted (especially in England), but its use was critical to the acceptance of infinitesimal calculus. Leibniz's notation is still, for the most part, in use today.

The success of mathematical sciences and the corresponding failure of natural history sciences—both taxonomical and encyclopedic—correlated to a splintering of research and development on cryptography. By the end of the seventeenth century, all the strange notations and hermetic forms of plaintext had effectively come to an end, but the development of cryptography did not stop—far from it. People started seeing cryptography as part of mathematics: first with cryptanalysis (long associated with statistics);[39] then, after the seventeenth century, (combinatorial) mathematics was increasingly used to calculate cryptographic strength; and eventually, mathematics became a core (if technically non-essential) aspect of encryption itself. The high point of this mathematization of cryptography, as described in chapter one, was the research and development in the twentieth century. During World War II, Shannon used mathematics to prove the possibility of perfectly secure cryptographic communication, and then, with the introduction of public key cryptography in the 1970s, a special mathematical function was placed *within* the encryption process. With public key cryptography, mathematics became the engine of the cryptographic system in ways never before seen. The result is that, today, cryptography is united across computer engineering, that investigates and perfects issues of security, and theoretical mathematics, which studies methods for breaking and making mathematical theorems relevant to the development of cryptography. Thus, from the humble origins of mathematical notation, the practical use of mathematics to create, manipulate, and ultimately understand cryptography led to the increasingly persistent instrumentalist view of cryptography.

Mathematical notation by itself, however, cannot *do* much. Mathematics, in the sense of calculations and proofs, offers powerful forms of abstraction and epistemic access, but as a set of techniques, it is limited. To significantly impact the real world—calculate logistics for shipping containers, serve online ads, and so on—mathematics needed to be corralled into concrete sets of rules, as algorithms. These algorithms, then, were energized by fast and powerful "computing" machinery, which could work on myriad inputs to calculate myriad outputs. The active ingredient, more often than not, was not a particularly

[39] For the Arab origins of statistical cryptanalysis, see chapter nine.

mathematical one (at the very least, rarely are the mathematics used in the digital world very sophisticated), rather, the algorithms that shape the world most profoundly are largely data driven and processual, using notational arrangements of the world. When this process was finally perfected, however, notational technologies took over from the previous discourse networks. The previously powerful discourse networks of writing and literature, mimetic in their origins, were left to play a secondary role to a new notational discourse network.

5.4 Discourse Network 2000, and the Rise of Algorithms

The discourse network circa 2000 can be characterized as the gradual rise of the influence of algorithms. Kittler himself only occasionally referred to the post-World War II development of the computer algorithm as being essential to the current discourse network, although commentators since have been more forthcoming in their willingness to historicize the present. Liu, for instance, argues that the discourse network 2000 is a synthesis of the two prior ones: updating the origin of meaning from the discourse network 1800, with the untranslatable, random selection and transposition channels of the discourse network 1900. Liu argues that the phenomenologically senseless "automatism" of contemporary discourses "follows from a precursor act of sense making" in apparatuses beyond direct human control.[40] This characterization fits well with how sense and nonsense interact in contemporary cryptography: human meaning making, in the form of textual representation, is quickly swallowed up as prepared plaintext is encrypted and made into ostensibly nonsensical ciphertext.

Most of the essential features of the history of plaintext within the discourse network circa 2000 can be traced to Hermann Hollerith's tabulating machine, first developed in the late 1880s, which I explored previously with Takhteyev.[41] Compared to the science fiction machines being discussed at the same time, which were imagined to transmit realistic likeness across space and time, the tabulating machine does not appear to have captured much of the speculative imagination of its contemporaries. Takhteyev and I argued that, for example, the science fiction author Albert Robida imagined a "telephonoscope," that

[40] Liu, *Local Transcendence*, 235.

[41] An earlier version of this argument was developed in DuPont and Takhteyev, "Ordering Space: Alternative Views of ICTs and Geography."

worked like the live television broadcasts or videoconferencing, which were actually developed later.[42] Unlike the mimetic functions of the telephonoscope or television, the tabulating machine possessed significant notational powers that would later underpin, and in fact, enable, many of the algorithmic technologies of the discourse network 2000.

Hollerith's tabulating machine was essentially a device for counting and sorting punch cards—sheets of paper marked with perforated holes, an idea inherited from textile looms. As I explored with Takhteyev, in the first use of the Hollerith tabulating machine, each card represented a household recorded by the 1890 census. While the punch card purposely provided a very limited representation compared to the richness of the mimetic image, its power lied in the fact that such representations can be processed in an automated and efficient way. With the earliest tabulators, the primary form of processing involved counting holes on the card and performing basic sorting (in locations where the holes were punched, pins connected and closed an electrical circuit, which the accumulator registered as mathematical addition). This ability to process the coded representations made the tabulator work, unlike abstract mathematics, in the sense of actually being able to do things in the world.

The purpose for which the tabulator was built is also indicative of the later use of algorithmic systems. The census office would use the machine to order representations of the population as a step towards eventually exercising control over the actual population.[43] Takhteyev and I argued that the re-ordering of notations on cards was a step towards "re-ordering," or even *controlling*, represented people. And while in the early years the gap between the two orderings was sufficiently wide that computational reordering of people could seem like a mere metaphor, in the years that followed such systems were used to identify, gather and dislocate or exterminate specific subsets of the population.[44]

While algorithms are not the only element of today's "control society," they are its essential component.[45] When the material world is ordered it can be used for disciplining or controlling subjects. Computers, therefore, become ideal tools of discipline and control. For example, socially sorting people can be performed for customer, credit, and crime profiling, often for commercial or

---

[42] Ibid.
[43] Luebeke and Milton, "Locating the Victim: An Overview of Census-Taking, Tabulation Technology and Persecution in Nazi Germany."
[44] Lubar, "'Do Not Fold, Spindle or Mutilate'"; Luebeke and Milton, "Locating the Victim: An Overview of Census-Taking, Tabulation Technology and Persecution in Nazi Germany."
[45] Deleuze, "Postscript on the Societies of Control"; Beniger, *The Control Revolution*; Pasquale, *The Black Box Society*.

discriminatory ends. Less nefariously, and perhaps more obviously, algorithmic technologies affect our daily experiences by facilitating the movement of material objects.[46] One such version is described by Kitchin and Dodge, who show the extent to which software underlies today's air travel infrastructure, resulting in a fusion of software and space that they term "code/space."[47] They argue, for example, that an airport check-in area is a code/space because if the software running the check-in process fails, the space stops being a check-in area at all.

It is important to note that the mimetic use of new media, in contrast to algorithmic uses, has also been historically important for many industries and applications. In fact, many important examples are "digital" (and therefore technically "notational") but remain mimetic in use. For example, while pilots may use voice transmission technology to communicate with dispatchers, rely on digital maps to identify their location, or pilot the airplane using fly-by-wire controls, these uses are fundamentally mimetic.[48] Nonetheless, Takhteyev and I argue that it is the algorithmic uses that enable some of the most dramatic recent changes. Many other elements of air travel, for example, utilize algorithms to manage the automated ordering of abstracted representations, and these are the most important ways of understanding contemporary technologies.

One example of the way that algorithms impact daily life is how books are purchased and delivered on Amazon.com (and similar companies).[49] From the customer's perspective, the process starts with an interest in buying a book. Amazon's website presents the customer with a ranked selection from a vast store of representations of books. The customer's purchase is registered in the database and then routed to a distribution center. This routing process aims to minimize the cost of processing and delivery by considering the location of the customer and the items, as well as the customer's other purchases. The order, then, may be split between multiple distribution centers depending on stock levels or calculated shipping distances. Alternatively, execution of a shipment may be strategically delayed to make it possible to aggregate other items for shipment.

Within the distribution center, orders are packed by a range of connected technologies: human employees who receive orders on handheld computers,

[46] DuPont and Takhteyev, "Ordering Space: Alternative Views of ICTs and Geography."
[47] Kitchin and Dodge, *Code/Space: Software and Everyday Life*.
[48] DuPont and Takhteyev, "Ordering Space: Alternative Views of ICTs and Geography."
[49] These examples are drawn from Ibid.

robotic shelving, as well as old-fashioned technologies such as forklifts moving palletized goods. As items are picked, packaged and shipped, each step is accompanied with an item identification scan to ensure that the representations are updated with the latest status information and tracked. The delivery of the shipments is normally handled by a different company, which uses its own technology for optimizing delivery and status tracking, but typically integrates with Amazon's systems.

The combined effect of algorithmic ordering in the case of Amazon.com is the dramatic reduction of delivery time and cost to a point where getting a book from Amazon can be both cheaper and faster than going to a local bookstore. More recently, Amazon has been transitioning to the use of smaller and more localized distribution centers, which has made it possible to further reduce delivery times and to start experimenting with selling perishable items, such as fresh groceries and last-minute items. Timely processing of such orders necessitates yet more complex computational ordering.

Another example of the influence of algorithms in daily life can be seen in the reconfiguration of work environments. As Takhteyev and I described, such computational environments may resemble mimetic systems, and in practice no bright line can be drawn between mimetic and algorithmic environments for many cases. Yet, by paying attention to the role of notation and algorithms, in principle, an important analytic difference is revealed. For mimetic environments, supporting interaction across space or time is often one of the main design objectives. Consequently, they are often judged by how close they come to replicating the gold standard of communication—face-to-face interaction. Algorithmically-driven environments, on the other hand, typically offer benefits derived from automated ordering and manipulation of representations, which cannot be achieved in face-to-face communication.

The Github system is an important example of an algorithmic work environment, providing an assemblage of computational services that facilitates modern software development. The most important service offered by Github is a revision control system called "git." Like other similar systems, git keeps track of modifications to software code, facilitating collaborative software work. Building on the idea in earlier systems, git provides strict identity for revisions, made possible by cryptographic message digests, or hash signatures.[50] The

[50] Hash signatures can be calculated without using cryptographic tools, but the cryptographic variants are an extremely popular and powerful use of cryptographic fundamentals. Despite their utility and power, hash signatures and hashing functions are sufficiently distinct from the kinds of cryptography under discussion here that they require separate treatment.

careful management of identity is what makes it possible to keep track of revisions, even as they are re-ordered or moved between subprojects. Due to the careful management of revisions, git also provides powerful mechanisms for automatic merging of revisions coming from different branches. These capabilities of identity management and performativity enable git to order and control software work.

Although useful for supporting remote collaboration, revision control and bug tracking systems were not developed with this intention per se. Early versions of such systems were, in fact, used by collocated work teams.[51] Such systems were adopted for their algorithmic benefits: they made it easier to keep track of units of work, rearrange them (automatically), and to associate bugs and revisions that address them.[52] At the same time, the effect of such systems has been to move the locus of software work from physical environments to computational ones, setting users and code into relations mediated by computing technologies.

While the Github system is algorithmic at its core with elements of mimesis, Takhteyev and I argued previously that Facebook provides an example of an environment that would be better described as a hybrid of algorithmic and mimetic uses of new media. Many of the interactions between Facebook users ("friends") are conducted using natural language or images and create a strong sense of presence. Such interactions establish strong markers of familiarity and sociality, creating an environment that Harrison and Dourish might call a virtual "place."[53] At the same time, however, Facebook presents a powerful and profound example of the algorithmic use of new media. The earliest version of Facebook functioned primarily as a database aiding users to meet new people. In this sense, Takhteyev and I point out, Facebook was algorithmic from the beginning. As mimetic features were added later, they remained embedded within the larger algorithmic context. Facebook does not merely group user content into topical or community-based sets. Rather, it presents each user with a unique ordering of content based on a model incorporating social relationships, privacy settings, and each user's preferences.

Much of the power of Facebook arises from mimetic and algorithmic elements working together. Facebook offers users a strong sense of presence: feeling as though interactions occur with real friends, privy to intimate or even mundane moments. Yet, in ways not usually made visible (unlike Github, the

[51] Naur and Randell, *Software Engineering*; Ambriola, Bendix, and Ciancarini, "The Evolution of Configuration Management and Version Control"; Ruparelia, "The History of Version Control."
[52] DuPont and Takhteyev, "Ordering Space: Alternative Views of ICTs and Geography."
[53] Harrison and Dourish, "Re-Place-Ing Space."

machinery of Facebook is almost completely opaque), these "intimate" moments are highly managed, controlled, and ordered. This ordering creates an experience that is in some ways more powerful than face-to-face interaction. For example, it makes it possible to maintain social contact with hundreds of people with nuanced degrees of engagement.

The algorithms are also crucial to Facebook's ability to monetize its business through advertising. While traditional advertising techniques are often mimetic, focusing on giving the viewer a sense of presence in the idealized world painted by the advertiser, modern advertising techniques used by companies such as Facebook and Google rely heavily on algorithmic matching of users and advertisers' messages. Abstracted representations of users and ad bids are entered into automated instant auctions, conducted in the milliseconds it takes for the browser to load a page. Facebook and other new media companies use powerful computational resources to actualize representations, finding hidden relationships and creating new insights to better link advertiser and consumer.

Behind these algorithmic technologies lies a powerful form of representation. Without a precise and unambiguous way of representing objects, algorithms would be useless or impossible. These algorithmic examples require a new way of thinking about their influence, and their forms of mediation. This new way of thinking is also required to understand the role of cryptography in the discourse network circa 2000. With the new media of routing algorithms, Facebook status update management, and ubiquitous cryptography—there lies, behind these algorithms, notation.

Despite the fact that the tabulating machine was real and was being put to widening use since the 1890s,[54] it failed to capture much interest by humanities and social science scholars. Similarly, when digital computers—in many ways the descendants of the algorithmic technologies of the nineteenth century—came to be studied by humanities and social science scholars, it was largely for their ability to support mimetic uses, not notational or algorithmic ones. Yet the algorithmic uses of computing technologies today are having as significant—quite possibly more significant—impact on our daily experiences than the mimetic uses.

5.5 Whither the Discourse Network?

According to the story, Zeuxis painted grapes with such skill that

[54] Austrian, *Herman Hollerith: Forgotten Giant of Information Processing*; Campbell-Kelly, "Punched-Card Machinery"; Cortada, *Before the Computer*; Yates, "Early Interactions between the Life Insurance and Computer Industries."

> *birds began to fly down to eat them from the pained vine.… [Today] the creation of illusions has been delegated to optical and electronic machines.*[55]

In the late 1990s, a great deal of scholarly attention was paid to virtual reality, in large part due to increased sophistication of display and computing technologies (two decades later, interest in virtual reality has resumed, as new commercial products have entered the market). One of the scholars paying close attention was Lev Manovich, who, for example, offered an account of the "RealityEngine[,…] a high-performance graphics computer that was manufactured by Silicon Graphics Inc. in the last decade of the twentieth century A.D."[56] This machine, Manovich argued, competed so effectively with the painted grapes in the myth of Zeuxis, described in this section's epigraph, that the "reality effect" which resulted was capable of extending its presence beyond the merely visual—convincingly making use of touch, hearing, and various forms of feedback.

What we have learned since the 1990s, however, is that the technology needed to create convincing alternative worlds is very difficult to produce. We discovered that the human brain is extremely sensitive to phantasmagoric experiences, and while it can at times be "tricked" into thinking a fabricated reality is (more or less) real, even the smallest parallax can ruin the illusion (going so far as to cause physical nausea in many people). This is because virtual reality is a kind of moving, immersive image, and as such requires extremely fast and sophisticated computational resources in order to make realistic-looking experiences. Unfortunately for virtual reality enthusiasts, as Kittler remarked, "computers, as they have existed since the World War II, are not designed for image-processing at all."[57] It has taken half a century since the first graphical programs were available to create virtual reality experiences that are convincing enough to be accepted in a commercial setting, and there is still a long way to go before these experiences produce a convincing simulacra.[58]

Yet, for all the challenges and hopes of creating a perfectly illusory experience, lower fidelity technologies can be powerfully mimetic in the right context. With its poor graphics (even for the time), slow response time, and unbelievable landscapes, the virtual world Second Life briefly captured our imagination, and

---

[55] Manovich, *The Language of New Media*, 177.
[56] Ibid.
[57] Kittler, *Optical media*, 226.
[58] See chapter ten for a description of the history of non-mimetic computer graphics—a remarkably distinct history from that of virtual reality—beginning with Sutherland's development of Sketchpad in 1963.

ushered in a flood of optimistic journalism and academic study. Second Life allowed the use of avatars that varied in the degree of resemblance to the people that were experiencing a "second life" inside the virtual environment. Despite these deficiencies, Second Life still created an important sense of "presence" for the users, a topic vigorously explored by research.

This continuum between high-fidelity and low-fidelity mimetic experiences highlights the ways in which mimesis is primarily perceptual, which is why scholars in "screen studies" tend to pick up on metaphors of vision and hearing (our most immediate sense perceptions). Phenomenologically speaking, mimetic experiences tend to be powerfully hermeneutical, typically operating at the level of common, shared intuition. That is, we are able to fill in the gaps of interpretation left by poor mimetic experiences because we have existing comparisons to draw from (recall the lesson Aristotle offered about truly novel mimetic experiences with no ready comparisons, which can still be educational or pleasurable, as I described in chapter three). Screen media, such as television or film, are fundamentally similar to painting, which tend to use certain cultural signs and conventions that "make sense" to a wide range of people (but not all peoples, at all times). These conventions are so natural-seeming and powerful that we often equate representation itself with the mimetic view. We usually think of lower fidelity (less clear) representations as "less" representational simply because they run counter to these assumptions.[59]

There is, however, another way to think about new media—one more fitting to today's discourse network. As I explore below, the more fitting way of thinking about new media focuses on computation and algorithms, in a broad sense. Since (and despite) Manovich's early and influential work, versions of this new view have been increasingly explored, especially in media studies,[60] but also human geography[61] and cultural studies.[62] Yet, the boundary between the two views has not been clearly articulated, and the analytical distinctions have not been fully explored. The distinction I draw, first explored with Takhteyev,[63] focuses on the use of new media to algorithmically reorder, rather than just transmit, digital representations. My specific contribution within these newer

[59] This mimetic view can be usefully compared to Kittler's discourse network 1800, when we saw considerable investment of money, time, and effort in developing technologies for hermeneutical meaning-making.
[60] Hayles, *Writing Machines*; Galloway, *Protocol*; Chun, *Programmed Visions*.
[61] Thrift and French, "The Automatic Production of Space"; Zook and Graham, "From Cyberspace to DigiPlace"; Kitchin and Dodge, *Code/Space: Software and Everyday Life*.
[62] Cheney-Lippold, "A New Algorithmic Identity"; Pasquale, *The Black Box Society*.
[63] DuPont and Takhteyev, "Ordering Space: Alternative Views of ICTs and Geography."

views is to focus on the utility of thinking about notation within algorithmic reordering and computation.

Over the last century, "media" have become important topics of scholarly pursuit. In particular, echoed in Manovich's theory, newer "mass" media technologies such as television, radio, and film captured the imagination of a generation of scholars, from Adorno to McLuhan, and many others still today. In this era, media culture was characterized by mass media technologies that were usually top-down and broadcast. Many aspects of these technologies could be traced to older media technologies with different logics, such as the book or the photograph. From the 1950s onwards, however, information and communication technologies powered by computers—which were eventually networked—started to change the media landscape in a significant way, quite unlike the media that came before.

Despite scholars studying mass media, from these early days of computing, cryptography was an explicit area of research and development within the field of computing. So tight was the connection between computing and cryptography, in fact, that Shannon's early work on information barely distinguishes between mathematical theories of information and mathematical theories of cryptography;[64] and Paul Baran's model for inter-networked computers in the early 1960s, for example, located cryptography in the center of the network, technically encrypting and decrypting within the same device responsible for packet-switching.[65] Now, a few decades after these early examples, computational and informational technologies today are "new" media,[66] and arguably dominate the contemporary media landscape. Of these new media, cryptography is not only an essential—perhaps even defining—aspect, it is one of the most politically contentious and actively discussed technologies today.

Why, then, has cryptography not received *any* attention by media scholars? Perhaps more than any other single book, Manovich's *The Language of New Media* is responsible for the direction of scholarship on new media today.[67] While Manovich's work was certainly not the first of its kind, it was a widely published and relatively accessible book that encapsulated the exciting and

[64] Recall the discussion from chapter one, where I cite Shannon's own admission that the information and cryptography problems are largely the same.
[65] See chapter ten for a description of the co-development of computing resources, especially networked ones, and mid-twentieth century cryptography.
[66] The newness of "new" media can be questioned, even if it is undeniable that something new has occurred due to technological advances. See Chun and Keenan, *New Media, Old Media*.
[67] Manovich, *The Language of New Media*.

complicated world of new media in familiar terms. In it, Manovich traces the movement from cinema to new media, arguing that "the accounts of realism developed in film theory can be usefully employed to talk about realism in new media."[68] Indeed, his reference points for new media are primarily computer-generated images, films, and other screen technologies.

If we are to diagnose why cryptography has been left out of the discussion of new media we must look at Manovich's book. Manovich focuses on familiar examples from drawn from screen studies, and the ancient theory of mimesis is used to explain how computational technologies are thought to work. Moreover, Manovich makes no mention of cryptography within the pages of *The Language of New Media* (although, in his defense, no other media theorist attends to cryptography either), but he also omits any serious discussion of the underlying computational and analytical technologies that surround us today. Instead of discussing how Facebook's algorithms work, for example, Manovich turns to the parallels between cinema and Photoshop or video games, and narrative and databases, and the flâneur and web browsing. These "icons of mimesis"[69] have framed what gets attention in subsequent new media theory, and have been important for developing an orthodoxy about how we think about new media technologies.

The colossal impact of computers, in my estimation, has not and will not come from remediating mimetic forms of expression. As we saw with the example of Facebook, social relations have changed in dramatic ways: people are now able to keep in touch and relate in ways that would have been unheard of before. Selfies, sexting, snaps, and foodgramming are now a regular part of life in "social media"—and these new remediations are not fundamentally mimetic in nature. In fact, the relationships (re-)mediated by Facebook are almost entirely due to the data points Facebook is able to collect and process.[70] The best accounts of these systems, in my opinion, recognize that our subjectivities are interpellated through stealthy algorithmic processes, which are processes that work most efficiently without the need for affective and mimetic representations.[71] Modern-day moralists, worried about the "influence" of mimetic technologies (so many screens), like those of Plato two thousand years

[68] Ibid., 198.
[69] Ibid., 195.
[70] Although the term does not seem to have resonated in wider literature, Kitchin and Dodge call these data points "capta," highlighting the way data have been selected and captured; Kitchin and Dodge, *Code/Space: Software and Everyday Life*.
[71] See, e.g., Berry, *The Philosophy of Software*; Chun, *Programmed Visions*; Pasquale, *The Black Box Society*.

previously, fail to comprehend the extent to which secret algorithms dominate life in the discourse network 2000.

New media, according to Manovich, are not fundamentally digital. Manovich argued that "although… [the principles of new media] are indeed logical consequences of digitization, they do not apply to concrete computer technologies in the way in which they are currently used."[72] Manovich's provocative claim is an attempt to resist the long-standing mathematics and engineering tradition that has understood new media in terms of its digital technology alone (which, in chapter one, I diagnosed as instrumental rationality). Manovich's reorientation of the study of new media away from these narrow instrumentalist constraints is important and necessary work, and as a result he opens the field to fruitful comparisons across disciplines and topics. As useful and necessary as Manovich's corrective was, however, his solution, focusing on connections to mimetic technologies, ended up also obscuring the effects and impact of many technologies that do not have screens, or that do not directly produce affect—that is, obscuring the role of so many invisible algorithms. As a consequence, among many other important technologies, cryptography was naturally excluded from the field of study.

I am not the first to have noticed Manovich's influence on the field, nor his preference for encapsulating new media in terms of mimetic cinema. In fact, Galloway calls Manovich's reliance on cinema the book's "dirty little secret."[73] Encouragingly, since the publication of Manovich's work, a small subset of scholars have addressed some of the errors, lacunae, and omissions—discussing, e.g., Facebook[74] or even the Java programming language[75] in terms that make more sense to their origins and functioning. Despite these insipient changes in the field, as of 2012, Galloway was *still* able to convincingly argue that "many scholars today continue to classify the computer as another installment in the long march of visual [i.e., mimetic] culture,… *such a position is totally wrong* [my emphasis]."[76] I have no doubt that the field will continue to improve and grow, interpreting newer and more complicated computational technologies in ways that do not succumb to mimetic thinking. Nonetheless, this chapter is one such attempt to understand new media without reference to the theory of mimesis, which also, and more specifically, shines a light on the how and why that cryptography had been left out of the existing literature.

---

[72] Manovich, *The Language of New Media*, 52.
[73] Galloway, "What Is New Media?"; Galloway, *The Interface Effect*, 4.
[74] Kember and Zylinska, *Life after New Media*.
[75] Mackenzie, *Cutting Code*.
[76] Galloway, *The Interface Effect*, 17.

5.6 Notation: A theory of plaintext

Plaintext is notational writing that is potentially encrypted. As such, plaintext is a vector, writing that points towards encryption, or, a "performance" linking a plaintext mark with ciphertext. In part two I describe how encryption is a further extension of notational logics, and I offer descriptions of the complex array of uses it has been put to over its long history. For the conclusion of part one, however, I provide a description of the analytical requirements of notation, drawn from Nelson Goodman's *Languages of Art*. These criteria determine what systems of writing can be considered notational, and therefore, what systems of writing can be called plaintext.

Up to this point I have discussed "notation" as though it is a univocal term. There are, in fact, notational *schemes* and notational *systems*. A notational scheme is a special kind of writing with very particular identity requirements. A notational system is the application of a notational scheme to a "performance," or a potential performance. Thus, a notational scheme is purely syntactic, while a notational system is syntactic *and semantic*. Since a notational scheme is a very particularly constrained set of marks, but it cannot by itself "do" very much. A notational system requires a performance in the sense of some (real or *imagined*) human-originated action (this can be a machine used by humans). Only once a set of marks is semantically associated with something—once they represent something in a particular way—can they become a notational system and acquire the additional set of representational powers of notation systems. Plaintext, then must only conform to the formal requirements of notational *schemes*. When plaintext is linked to ciphertext through a performance of encryption, however, it becomes a notational *system*, that is, encryption forges a special "semantic" link between plaintext and ciphertext.

Common notational schemes include the alphabet, binary encoding, Morse code, and musical notation. The simplest of these is binary: the most basic distinction possible, said to be a primeval cleaving of lightness from darkness, good from bad, up from down, yes from no, and one from zero. The key to what makes binary *bi*nary is the *difference* between the marks.[77] This basic

[77] Digitality is a subset of notation. Given the enormous role "the digital" plays in contemporary life, it is worth considering how "analog" technologies fit within this narrative. There are in fact many kinds of "analog" computers, varying in form, from some of the first machines used for rapid mathematical analysis (particularly useful for calculating differential equations for gun direction and targeting, as Vannevar Bush developed in the 1920s), to operational amplifiers. Analog computers also come in many different material configurations, making use of electricity, fluids, gears, balls, and slides. Although not as common today, analog computers

requirement of difference is common to all notational schemes. The alphabet, recall from the previous discussion, is notational because the mark <a> is different from the mark <b>. As Kittler noted, there is an "optical" character to notation, because identifying such differences is most easily accomplished with sight.[78]

The set of differences required for a notational scheme can be loosely called "discrete." In this chapter I will be more precise and follow Goodman's terminology, describing differences that are "disjointed" and "finitely differentiated." The development of a notational scheme involves creating constitutive criteria that are characterized by of disjointedness and finite differentiation—that is, any marks or inscriptions must have these properties in order to belong to a "character" (an element in the scheme). Fundamentally, disjointedness and finite differentiation enable a character in a notational scheme to be freely exchanged for one another without syntactic effect. For example, the mark <a> can be replaced with another mark <a>, but similarly, also <A> or <*a*>.[79] Each of the marks must be, in Goodman's terms, a "true copy."[80] Using terminology more familiar to analytical philosophy, we can say that a notational scheme is a set of constitutive rules that specify that the token <a> can be replaced with another token <a>, together comprising tokens of a particular type.

Notice here, the visual outline of the marks need not be identical: as a, A, and $\mathcal{A}$ all look quite different. The only requirement for these marks is that they must all be "indifferent." "Indifference" means the mark <a> belongs to the same class as <A>, but both are excluded from the class <d> (and <d> is correspondingly excluded from the class <a>), and this must hold for all possible marks in the notational scheme. This also means all characters must be "disjoint."[81] Characters are disjoint when a class can be established that all characters of the type "the letter a" excludes all other non-compliant classes (that is, classes that lack this property). Therefore, in the notational scheme

---

have many potential benefits over digital ones, as they are *in theory* infinitely precise and instant. However, analog computers lack the benefits of notation.

[78] There is no formal requirement that notation is expressed materially, or sensed with vision, but merely imagining a notational system is not very useful, and hearing or touching or tasting notation can prove challenging, but is certainly not impossible. The Morse code telegraph system, for instance, is as much visual as physical and auditory, with users tapping out messages by hand using loud actuators.

[79] Goodman, *Languages of Art*, 131, 133.

[80] Ibid., 131–32.

[81] Ibid., 133.

considered here, there is no overlap in the sets of characters between <a> and <d>, as *plaintext*.

In fact, this requirement of disjointedness must be held in theory, even if in practice it may be hard to determine. For example, a smudged <a> might look like a <d>, which means it is a judgement call whether or not the given mark is compliant with "the letter a" class. As Goodman notes, when designing a practical notational scheme it is an important engineering challenge to ensure that such edge cases do not occur too often (that there is not too much smudging), since frequent ambiguity would cause a breakdown of the system and its goals. It is, for example, better to design a binary electric circuit where the cutoff between the notations 0 and 1 is large enough to be reliably determined, perhaps a scheme where voltage <0.01=0 and voltage >5=1, rather than a scheme where voltage <0.000001=0 and voltage >0.0000011=1. In both cases the notational scheme is disjointed, but the latter would be difficult to reliably use without very precise measurement techniques.

The notational scheme must also be finitely differentiated.[82] That a mark cannot belong to two different character classes must be determinate finitely. For example, an analog clock has divisions for minutes, but if the clock is to be read in a way that between each minute marker the hand "approximates" the time as it sweeps through the minute, then the scheme is not finitely differentiated, and therefore not a notational scheme.[83] If, on the other hand, time is only read once the hand is past the marker (the process of determining when the hand is past the marker is sometimes practically troublesome—best to use thin lines on a clock that is going to be read notationally), then the scheme is finitely differentiated (and disjoint), and thus a notational scheme.

As the clock example makes clear, a notational scheme can be constructed out of anything, but how we decide to interpret the marks makes all the difference. What we lose in precision when we decline to read the clock between the minute marks (no longer able to say "the time is 3:05 and (about) 10 seconds"), we gain back in being able to better order, manage, and manipulate the clock readings. For instance, "counting" time notations is possible because the "true" time is ignored.[84] The very idea of dividing the *actually* smooth flow of time, first into daytime and nighttime, and then into regular intervals—hours, then

[82] Ibid., 136.
[83] Ibid., 157.
[84] In fact, our experience of time is never "true," as Augustine identified in his paradox about time: there is no "present" because in speaking of the present the present has already become past, there is no past because it is already past, and there is no future because it has not yet come.

minutes, then seconds, and so on—was a historical stroke of genius for productivity and capitalism. Such thinking seems natural today, but for those without clocks, its introduction must have seemed foreign.[85] Perhaps as foreign as a person today who might marvel at how the computer is able to do so many things with, as they say, just "ones and zeros."

When a notational scheme is associated with a some special "performance," it becomes meaningful in a new way, as a *notational system*. Notational systems are much less common than notational schemes because they have rigid semantic requirements. Whereas a representational scheme is free to establish any number of marks or utterances that refer to a given object in the world (as if by decree, which is why translation across languages works), the marks in a notational system must relate *directly* and *univocally* to *its* world (not necessarily "the" world—the referent may be ideal or constitutive). In fact, the process of establishing a notational system typically requires a considerable amount of sophistication to make the particular notational configuration make *sense*.

As described above, plaintext is a special kind of human expression that conforms to the formal requirements of syntactic "disjointedness" and "finite differentiation." In part two, I describe the rich processes of *encryption*. Importantly, there is a system of notation underpinning all three schemata of cryptography (plaintext, encryption, ciphertext). That is, the notational system provides the formal requirements for how plaintext is linked to ciphertext, a performance that shifts the analysis from a notational *scheme* to a notational *system*. For encryption, a notational *system* is a kind of reflexive and inward-looking system, which creates a compliance class between notational schemes. That is, encryption is the "semantic" process of making a compliance class between the notational scheme of plaintext and the notational scheme of ciphertext (such that, e.g., the letter <a> is compliant with the letter <d>). I will now briefly discuss the formal requirements of notational systems as they apply to the performance of encryption.

Notational systems must not have marks that are "vacant," or without a compliant (empty), but more importantly, they must be *unambiguous*, and *semantically disjointed and finitely differentiated*. This means that ordinary language is not a notational system (even when written in a notational scheme, like an alphabet). Goodman offers the example of "doctor," "Englishman," and "man," which cannot be part of a notational system in English because these are

[85] This experience first occurred in Greek and Roman times, even though the sundial had existed since the Egyptians. See Mayr, *Authority, Liberty & Automatic Machinery in Early Modern Europe*.

semantically intersecting terms.[86] If the notational system contains the term "man" it cannot contain the more specific term "Englishman" without introducing overlapping sets (and destroying the requirement of semantic disjointedness). Similarly, Arabic numerals representing physical objects (e.g., counting pebbles in a river) cannot be a notational system because there is no in-principle limit to the compliance set (which destroys the requirement of semantic finite differentiation).

Thus, there are two conditions for notational schemes and five for notational systems. A system is notational, Goodman summarizes, if and only if:

> *all objects complying with inscriptions of a given character belong to the same compliance class and we can, theoretically, determine that each mark belongs to, and each object complies with inscriptions of, at most one particular character.*[87]

Another way of understanding notational schemes and systems, and how plaintext is involved, is to compare Goodman's distinction between "artworks" (any utterances, marks, or inscriptions) that are fakable and those that are unfakable. Goodman calls unfakable artworks "allographic," and those that can be faked "autographic."[88] Plaintext is unfakable because the important fact about the marks or utterances of plaintext is their determinate order (since they are not just natural language, but potentially encrypted marks).[89] Order of (notational) marks is the relevant feature of plaintext.

Being able to determine whether a given set of marks or inscriptions is allographic or autographic requires understanding the given performance's contingent and constitutive properties. The constitutive properties of a painting are, for example, that it involves paint or perhaps has aesthetic properties (such as being beautiful, or having artistic merit, and so on). Contingent properties of the painting may include the fact that it is blue, that it was painted by Picasso, or that it was destroyed in a fire—in other words, the contingent properties are its history. The painting is, in its relevant (and important) qualities, autographic because the painting must always face the question that it may be a fake (a fake Picasso possessing the *relevant but contingent history* that it was not painted by Picasso). Even if we admit the science fiction example of a perfect atom-by-atom reproduction, the painting remains autographic. This is because there is no *in-theory* way to determine whether the painting under inspection is

[86] Goodman, *Languages of Art*, 152.
[87] Ibid., 156.
[88] Ibid., 113.
[89] See chapter ten for a discussion of the role of order.

authentic or fake. There are, of course, many practical and contingent ways to assess such a question, but worries about authenticity always remain for paintings because we lack a "test of compliance" to measure the performance against an ideal.[90] There is no such ideal, and thus the painting is not allographic, because it lacks the *constitutive* property of being comprised of an "alphabet of characters" (where "alphabet" is a set of appropriate marks).[91]

Indeed, it is clear that art is not just any paint on the wall, or clay formed in some haphazard shape, or human movement of any kind. What makes art important is that it has certain qualities (usually, but not always, thought to be aesthetic).[92] Autographic arts, such as painting, are typically understood as having aesthetic qualities in most or all relevant aspects, but of course, not always.[93] Allographic arts (unlike painting), on the other hand, may have (very important) aesthetic qualities but these properties are not *constitutive* of the work and thus not relevant to the fact that they are notational. For example, an orchestral performance of Bach may have many aesthetic properties (and is no less beautiful than painting or some other kind of autographic art), but *in terms of its notationality*, such *contingent properties do not matter*. Indeed, "correctness and quality" of the performance are not constitutive properties of allographic arts.[94] Correctness must have some threshold for determining whether a performance of an allographic work can rightly be said to be a "performance" of the specified "work," but such a determination is a practical not analytical matter.

A performance of a given work that does not meet some threshold of correctness with regard to the activity is not deemed a fake performance, but rather, is said to be a performance of a different work. For expressions that are deemed notational, the relevant properties of the performance are its relationship to the particular work (its music, its score), which are constitutive of the work, whereas, in the case of notational artwork, all of the aesthetic qualities are deemed contingent. For example, a music score is constitutive of its performance, and the ability to "correlate appropriate sounds with the visible signs in the score" define it as allographic.[95] Whether a given performance is

[90] Goodman, *Languages of Art*, 119.
[91] Ibid., 116.
[92] Young, *Art and Knowledge*.
[93] There is a loose alliance between mimetic and autographic arts; the imitative doubling of mimesis is formally compatible with allographic arts, but strains the core essence of mimetic art. With the introduction, below, of a distinction between notational schemes and systems it will become clear that the latter is not in any way compatible with the mimetic theory.
[94] Goodman, *Languages of Art*, 113.
[95] Ibid., 117.

beautiful, or played expressively, or loudly, is not constitutive of its performance. Even in the case where some of these qualities may be marked in the score (such as "allegro" or "adagio"), they are not properly speaking part of the notation. An allographic performance cannot be faked because we have a constitutive test to measure against an ideal—in the case of the musical performance, we have the musical score.

Unlike autographic art, allographic art is not concerned with the history of its production. Good or bad, a performance of a musical score qualifies as a performance of that score. The performance must simply be a compliant expression of the work. The identity of the "work" is constituted by being a true copy of the score, with no concern for whether the present version is an "original" in the composer's hand or a faded photocopy. Similarly, a performance from a photocopy should not be judged differently from one played from the "original," at least not in terms of its identity (the two performances may differ in many aesthetic respects, irrespective of the musical score). In terms of being a performance of a given work, works played from an original or a photocopy are identical.

The reason painting is autographic and musical scores are allographic is not due to some special arrangement of materials. A notational system can be developed for anything, with enough "force." Paint-by-number, or, some new kind of computer-controlled algorithmic painting, would be properly notational systems, but even if the machine were able to recreate a Picasso, few would be willing to accept that Picasso's masterpiece was, or even *could be*, reduced to a set of numbers or coordinates in a computer and not lose something vital to the art.

For historical and psychological reasons we do not feel the same way about most music. We do not feel that two different performances of Bach's masterpiece, *Goldberg Variations,* constitute different versions of the work,[96] even if we might prefer Glenn Gould's performance over the rough version played by a high-school student. Despite differences in performance, we still recognize both as being distinctively Bach. In terms of aesthetics, a beautiful performance of Bach matters, and we recognize that Gould's performance dazzles—indeed, it has been called the triumph of the "Gould utterance" over the "Bach utterance."[97] Despite these important aesthetic concerns, the

[96] Or Alberti's *Descriptio Urbis Romae.*

[97] Debray, *Transmitting Culture*, 106. There is a "second scheme" that bears witness to the stability of Bach, the way in which "we no longer hear Bach done by Gould but Glenn Gould in Bach."

notational properties that underlie Bach's musical score create the identity for the work; in fact, Debray asks, who remembers that the *Goldberg Variations* were originally composed for a two keyboard harpsichord?[98] In the end, Gould effaces himself before Bach—like an "illusionist carrying out a disappearing act"—we see Gould but hear Bach, as "a revelation, an encounter, a shock."[99]

Some arts, such as dancing, have a liminal position in terms of our psychological and historical willingness to accept them as notational. We might be willing at accept that a good notation system (and capable transcription) captures what is essential to dance (such as the acclaimed Labanotation system described by Goodman), but that a poor notational system does not. Yet some people may complain that a dance performed from notation is like a paint-by-number version of Picasso—that the performance itself must be constitutive of the art. Such people would demand that each time the dance is performed, we must consider the performance on its own, individual, merits—an acceptable, if rather high bar for identity in art. On the other hand, we might recognize that dance notation may not capture as many of the finer details of the art as musical notation, but then we should, perhaps, speak of a poorer notation with less "resolution" or "fineness," but not necessarily claim that dance is an autographic art.

We might similarly marvel at how the invention of writing became a historically accepted form of a notation scheme, seemingly capable of capturing the essential and vital aspects of such a complex thing as natural language. Recall the discussion of handwriting and type (from chapters three and four), which is in some ways like the fluid movements of a dancer. But, writing can also be considered an allographic art if the relevant (and constitutive) aspects are the composition of the letters themselves (perhaps in the way an illiterate person sees text, *not* in terms of the letters representing English or some other natural language). In fact, handwriting in an alphabetic script is, *in terms of notation*, identical to the printing press. A printing press, however, as we saw, makes the notational properties already present in the alphabet more obvious, and thus makes the theoretical connection between notation and the alphabet more obvious. For this same reason, musical notation, comprised of individual notes, developed much earlier in history than dance notation—it is somewhat more obvious that one can create a notation for music comprised of discrete notes than it is that one can do the same for fluid dance moves.

[98] Ibid.
[99] Ibid., 107.

So, alphabetic writing in a natural language (e.g., a written novel) can be considered allographic, and is comprised of a notational scheme—not a notational *system*—because the marks are disjoint and finitely differentiated, and the constitutive properties of the writing could be understood as being a true copy of the original (perhaps from some manuscript that has been printed, in the same way that a photocopy of a musical score is a true copy). That the writing expresses meaning in natural language, and this meaning is deemed important and constitutive, excludes it from being a notational system, since each word will fail the semantic tests of unambiguity and semantic disjointedness and finite differentiatedness.

Plaintext is, therefore, token identical to alphabetic writing in a natural language, but due to it being oriented towards encryption, it has a different set of constitutive properties. As plaintext, writing is reduced to an articulate set of characters and the relative positions for them. In principle, anything at all can be reduced in this way, but such a reduction may come at an unacceptable loss of important contingent properties—an important kind of representational violence. Therefore, plaintext is allographic and *potentially* autographic (plaintext that is potentially encrypted). The performance of encryption substitutes marks from one notational scheme to another, and in doing so suspends any *prior* meaning by linking plaintext to ciphertext, without semantic ambiguity. This is precisely the sense of "semantic" connection between plaintext and ciphertext that encryption constitutes. If the encryption is never reversed, the original meaning is lost. Moreover, in the very act of calling some writing "plaintext," we are signaling that the prior qualities of beauty, expressiveness, morality, and (natural language) intentional meaning are contingent and deemed unimportant (qua plaintext). For whatever contingent features ciphertext might also have, they are certainly not those of the original expression.

We can now see why anything can be plaintext, but the conversion process comes with serious consequences. Sliding further into the violence of *re-*presentation, as, for example, transcribing written words into Morse code—and beyond into ciphertext—may mean losing many qualities that are deemed important to the original utterance. In Morse code, the system of grammar, morphology, syntax, and pragmatics previously present in the original utterance are all replaced with the logics and identities of Morse code. Plaintext causes writing to gain and lose powers, as representation potentially shifts ineluctably away from the human, linguistic register.

Encryption then brings more, and different, logics—forcing a relationship to an Other not present in the original expression.[100] I argue that to fully understand encryption we must dissuade ourselves from the view that these acts are innocent. Perhaps the written marks do not change in their material shape or arrangement, but our view of them and their relationship to the world does, and therefore, I stress, they *do* change.

5.6.1 The representational violence of notation

Far from just an intellectual exercise, the actual creation and recognition of notational writing is a powerful, if natural feeling, form of expression. Indeed, without notation, cryptography would be impossible. Moreover, all "digital" computing would also be impossible—as would the complex ways of ordering and arranging the world using the technologies of new media. Without notation, most of the activities we simply take for granted in the developed West—from point of sale terminals at the grocery store to aircraft autopilot—would look and work very differently, if such processes were possible at all.

Notation is so useful because it is designed to ignore certain qualities and highlight others. This process is a form of abstraction, which is also a key feature of complex human thought. Returning to a previous example, when the Hollerith tabulator was used for ordering and analyzing census returns, the notational marks on the punch cards abstracted away the complexity of the people it represented. Grey areas, fluid change, and continuous gradations are all erased when represented notationally.

This process of abstraction is not without considerable violence—first as representational violence, then—often—with "real world" violence. The non-existence of gender fluidity for census data collected on Hollerith punch cards had real world consequences for many people. If a punch card only has room for Male and Female choices, respondents must conform to the *notational reality*. People who identify as transsexual must either choose one of the available binaries, or risk exclusion (that is, exclusions from social programs, political representation, and so on). Adding a third option, perhaps "transsexual," might alleviate the problem somewhat, but this is fundamentally a futile exercise. There are many other gradations and identities that are still not represented in this third choice, and such a stopgap merely extends the subtly of the underlying notational reality, rather than overthrowing it. This is a well-known

[100] See part three for a discussion of how writing is thrust into new relationships and has to encounter the Other.

problem with cataloging and sorting,[101] which is a result of bending and forcing the fluidity of the world into notational forms of abstraction.

Such a fact may appear at first glance obvious and non-problematic, but it has far reaching effects—being the first step away from humanity, language, and being. Cryptography reorients our relationship to language because plaintext *must* be notational. Consider Mario Savio's famous speech against the ways that students were being represented by the gears, wheels, levers, and apparatuses that sorted University of California, Berkeley students. Savio preached against the dehumanizing tendency of automated sorting and analysis: "But [if] we're a bunch of raw materials—that don't mean… [they can] have any process upon us." At the same time, one UC Berkeley student pinned a sign to his chest: "I am a UC student. Please don't bend, fold, spindle or mutilate me," reinterpreting the prohibition printed on computing punch cards.[102]

These protests resulted from fear of machines and labour automation, but they are also a general claim against the violence of notation. As Goodman astutely noted, questions of notation "reach deep into the theory of language and knowledge."[103] The punch card is just one stereotypical example and serves as a useful synecdoche for broader forces at play (see figure 5.2). Because it is notational, the punch card abstracts away qualities of humanity that are sometimes deemed important, and replaces them with semantic connections that seem alien or abhorrent.

[101] See, for example, Bowker and Star, *Sorting Things out*.
[102] Lubar, "'Do Not Fold, Spindle or Mutilate,'" 48.
[103] Goodman, *Languages of Art*, 127.

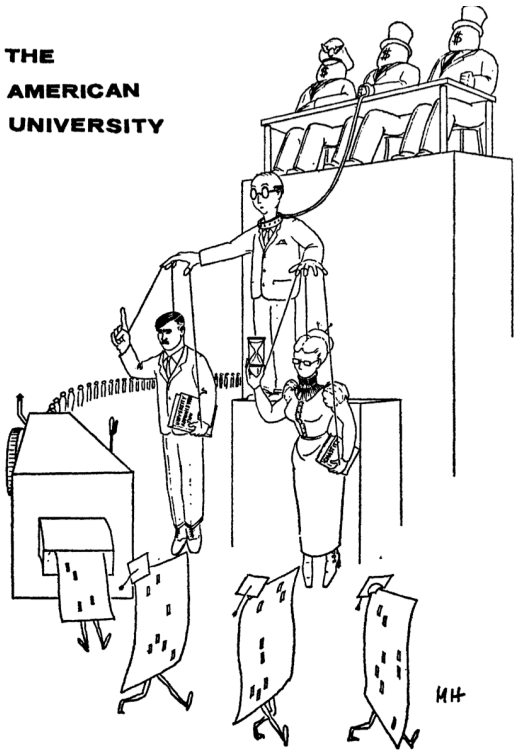


Figure 5.2: Political cartoon satirizing American universities, from W.E.B. DuBois Club newsletter.[104]

Cryptography goes even further in the same direction than the punch card's potentially false and inhuman abstractions: turning all writing into plaintext, in preparation for encryption that is *impossible* for humans to even *understand*. Once encrypted, such notational representations are completely opaque to humans, can only be processed by machines, and even when decrypted exclude interpretation by all individuals not suitably authorized. Yet today, there are no protests to throw ourselves upon the gears, wheels, and levers of cryptography.

❦

Given the political importance, it is surprising to see those on the political "Left," and defenders of individual and consumer rights, consistently line up for more cryptography—advocating ubiquitous cryptography so strong that not even government intelligence agencies can crack it.[105] We might place some blame for this confusion and apathy on scholars, who have systematically failed to problematize questions of what cryptography is. In my opinion, media

[104] Reproduced from Lubar, "'Do Not Fold, Spindle or Mutilate,'" 47.
[105] The Electronic Frontier Foundation has been at the forefront of this call to action, refusing to admit any potential compromises even when cryptography is being used in ways that affect national security, and is demonstrably in the interest of powerful companies, not individuals. See DuPont, "Opinion: Why Apple Isn't Acting in the Public's Interest."

scholars should have been on the front lines, but if my diagnostic is correct, they have traditionally missed making these important interventions due to deep-seated theoretical biases towards understanding mediation in terms of mimetic representation, at the expense of seeing pervasive forms of notational representation and algorithmic processing. Interventions may be coming, however, as critical code studies, software studies, and related fields begin to tackle codes of all kinds. Perhaps, in the future, these interventions will join the present work and focus on these ways of understanding cryptography.

Part 2: Encryption

In this part I rewrite the term "encryption." Chapter six is a transitional chapter, between plaintext and encryption; and in it I develop an approach to understanding cryptography in terms of code, and analyze a cryptographic case study using the approach. Chapter seven introduces the primal scene of cryptography, encryption which is a mediatic process, and I investigate how theories of perception were a way of understanding the material limits of encryption. Chapter eight develops a transmission model of encryption using a model and myth of angelic messengers. Chapter nine investigates the history of cryptanalysis and machine translation, finding that while there is an essential connection between the two, as a form of notational transcription, encryption has distinct ontological properties and processes.

6
Codes and codeworks

At the close of chapter five I suggested that scholarship ought to take seriously cryptography as an important topic, worthy of critical study. I suggested that critical code studies, software studies and related fields are well positioned to free themselves from the theory of mimetic representation that has traditionally dominated media studies, and in doing so, tackle codes—and especially cryptographic ones—in new ways. In this chapter, I transition from plaintext to encryption by focusing on "code," a broad, polysemic term often associated in popular discourse with cryptography, among other technologies. Despite the challenges of applying such a broad term to the narrow study of cryptography, the term nonetheless offers some illuminating associations, which are useful as my analysis transitions from plaintext to encryption. To this end, I introduce two descriptions of "code" that explicitly tackle cryptographic issues. The first, from Umberto Eco, describes cryptography in terms of semiotic code systems. The second, from Friedrich Kittler, associates a broad range of codes and code technologies with cryptography, collapsing the prior category into the latter. With Eco and Kittler's analyses of code in hand, I investigate the encrypted e-poem *Agrippa (a book of the dead),* as a broadly cryptographic digital humanities case study, which reveals the ways that code can be understood in explicitly cryptographic ways. This specific code artifact also exemplifies the way that plaintext is reconfigured in the presence of encryption.

In this chapter, I briefly depart from the archeological method I developed for understanding cryptography, and instead track some of the footprints of code as it is discussed in a digital humanities context, formally connected to software studies and critical code studies, and related fields. As such, I discuss how code functions in several contexts—as a social product, text, executable code, and so on. These views are distinct from the more typical interpretative stance of social scientists and humanities scholars studying the *effects* of cryptography, who tend to focus on how society functions *with* code. In these cases, cryptography is sometimes understood and uncritically leveraged to optimize functional goals, such as the desire for privacy or secrecy, even when these goals are at political and ideological odds with certain other values. In charting this alternative view of code, normative, social, and political issues are brought into view in new ways.

In recent years there have been a number of works that have managed to avoid both technical and functional, or socially-reductive, analyses, and instead have sought to understand how code becomes socialized and powerful, while also approaching code as a distinct, legitimate topic of study. Many of these works fly under the banner of software studies or critical code studies. While these fields have not yet begun studying cryptography, they have studied "code," a cognate topic. These analyses of code show interest in issues parallel to those I also present in the study of cryptography.

6.1 What is code?

There are many discussions of code by linguists and semioticians, but rather few of these scholars have much experience with or interest in the ways that code becomes actualized in machines. Ferdinand de Saussure—largely responsible for the modern study of semiosis—took seriously the existence of code, emphasizing the arbitrary nature of code (that a code can take on any value attributed to it), but did not discuss code in the context of machines. Somewhat more aware of machines and information theory, and also influenced by Saussure, Roman Jakobson thought of code in the context of the functional operation of messages, as part of a sender-receiver model of communication. As I will discuss below, Umberto Eco built on Saussure and Jakobson's model, believing code was a feature of semiosis within a theory that operates on Hjelmslevian content and expression planes.

Outside of linguistics and semiotics, the nature of code has been less frequently discussed, despite arguably being a feature of nearly all modern life and cutting across a vast number of academic disciplines. The obvious exceptions have been computer scientists and software developers, who use code every day and have good working *internalist* definitions,[1] but these explanations are limited in their explanatory power (typically positioning code within a context of instrumental rationality). This limited explanatory power is especially apparent when talking not about the broad category of code, but about the more specialized topic of cryptography, which promiscuously crosses between language to computation.

[1] Consider the Oxford Dictionary of Computing's definition: "A rule for transforming a message from one symbolic form (the source alphabet) into another (the target alphabet), usually without loss of information." The dictionary also offers more technical (mathematical) definitions that rely on one-to-one homomorphisms between sets. Such a definition shares some of the merits, and challenges, of Eco's definition. See Daintith and Wright, "Code."

Outside of linguistics and computer science, the descriptions and definitions offered by various software and critical code studies are, although sometimes lacking the precision of the other fields, somewhat better at capturing the fulsome nature of code. Here, the list of works describing code is rather long for such a young field—a product of efforts to define the field's central object of study (and the list of works dealing with code is much better than those dealing with cryptography). Beyond Kittler (whose influence is wide-reaching), one of the earliest descriptions of code in software studies was offered by Manovich, which I discussed in chapter five, and found wanting. In the years following, a number of other scholars begun to define and analyze code.

In the introduction to a special journal issue on code, Mackenzie and Vurdubakis problematize how code has been instrumentalized, and became associated with executable programs and mathematical algorithms. They argue that code's other senses—as a body of laws and regulations of subjects, or of the ways of communicating openly or in secret—still carry weight, despite often being overtaken and subsumed by more traditional analyses.[2] Mackenzie and Vurdubakis make a case for how the executability of code ought to be recognized as a form of performativity, much like how we understand natural language to be performative in certain circumstances. In the same special issue, Introna argues that we ought to understand the agency implied in code by interrogating it as text, opening up a large field of study (perhaps for the digital humanist?).[3] These works, and many others, seem to approach code on its own terms, and show how code moves through machinic and social contexts, sometimes with resistance, or sometimes imperceptibly. We would do well to further attend to the points of resistance and imperceptibility—the way we react against some codes, the way we fail to see others—that reveals something about code and our relation to it.

Adrian Mackenzie has emerged as a focal figure in software studies and frequently comments on the subject of code. In one of his early works, Mackenzie problematizes code, asking why code should be considered a topic of study at all, and under what terms we might study it.[4] He concludes that code offers an interesting range of problems. While we usually consider code to be a set of instructions that control the operation of a computing machine, Mackenzie shows that this is in fact an artificial stabilization. Mackenzie argues

[2] Mackenzie and Vurdubakis, "Codes and Codings in Crisis: Signification, Performativity, and Excess."
[3] Introna, "The Enframing of Code."
[4] Mackenzie, "The Problem of Computer Code: Leviathan or Common Power?"

that we should recognize that code can be understood as text and process—the prior being exemplified by stabilized source code, and the latter by executable code. In the transformation that occurs during code execution, as code vacillates between text and process, code becomes integrated and disintegrated, and (quoting Kittler) "appears to write itself" as it "evades perception" and hides.[5] In a later paper, Mackenzie returns to the question of code and again resists the tendency to rely on reductive or formal explanations of code, which isolate code from its particular contexts, reducing it to "culture" or the various "cultures of software."[6] Instead, Mackenzie "follows" code as it moves across a terrain of forces and agencies. Mackenzie frames code as an index to social agencies, sitting between its originators (software developers, webmasters, project managers, *etc.*) and recipients (users across all scales—from those who interact with the operating system kernel, to those who use a graphical user interface). Code, therefore, according to Mackenzie, is social and culturally specific.

Similarly, Marino's description of critical code studies suggests that we should critically interpret code as we would any other text. Marino also points out that computer code exists for multiple recipients—for the programmer, but also other programmers, and the computer itself (which, however, does not "interpret" the code).[7] The central problematic Marino tackles is whether we should study code as surface text, or as executable text. Marino reiterates the debates that have been present in new media art, especially "net" art. On one side of the debate, some authors believe that computer code is special precisely because it is executable. Such a position is held by Cayley.[8] However, Raley responds to Cayley, arguing that such a privileging of the output is deficient.[9] Raley believes that code can function more ambiguously, as when codeworks make visible the hidden operations of computation.[10]

Cramer also interprets code in terms of its executability, tracing this performative nature back through the Jewish and Christian Cabbalah and

[5] Ibid., 8.
[6] Mackenzie, *Cutting Code*, 4.
[7] Marino, Mark C., "Critical Code Studies."
[8] Cayley, "The Code Is Not the Text (Unless It Is the Text)."
[9] Note here certain apparent similarities between Adorno's "deficient" belief that music is a result of a score and the description of plaintext in terms of notation in chapter five. I believe my account avoids the worst errors of Adorno's simply because my description of plaintext in terms of notation is only part of the complex of cryptography. Encryption and ciphertext inherit notational properties, but are in no way exhausted by them. Encryption moves, hides, and transforms in many complex ways, explored in the following chapters.
[10] Raley, "Code.surface || Code.depth."

Renaissance theories of magic.[11] Cramer points out that much of this work owes its practical and theoretical impetus to Ramon Lull's combinatory Art, which we encountered previously (in chapter three), as it tracked through the Renaissance systems of representation. In a similar fashion, Thomas connects code to the human body in an effort to understand the ways that code is performative. Thomas interprets code as regulatory, following Lessig,[12] believing that code determines what is possible. It is precisely code's connection to writing, Thomas argues, where writing becomes alien—invisible but also "opaque, lasting and permanent," and therefore a "performance."[13]

Despite the extensive discussions of code—from linguistics, computer science, and software and critical code studies, and the many areas of obvious overlap—very few authors mention cryptography, and even fewer have made cryptography a central feature of their account. I am aware of only two descriptions of code that foreground cryptography: Eco's definition of code in *Semiotics and the Philosophy of Language,* and throughout Kittler's oeuvre, but especially his short article, "Code (or, How You Can Write Something Differently)."

6.1.1 Umberto Eco's definition of code

Eco suggests that cryptography is a kind of "code." In an effort to clarify the semantic ambiguity of the term, he specifies three senses of code: paleographic, institutional, and correlational. The latter correlation is the only properly cryptographic sense of code.[14] According to Eco, correlational codes are modeled after code books or dictionaries that provide a set of correlations between an inscription and a series of alphabetic letters. Eco argues that correlational codes are not so much a mechanism of communication as they are mechanisms to allow transformations between two systems. The mechanism of transformation is transcription, either in the form of transposition or substitution. According to Eco, "a cipher substitutes every minimal element of the plaintext with the element of another set of expressions."[15] Eco's definition summarizes all of these elements:

[11] Cramer, *Words Made Flesh: Code, Culture, Imagination*.
[12] Lessig, *Code and Other Laws of Cyberspace*.
[13] Thomas, "Hacking the Body."
[14] Eco, *Semiotics and the Philosophy of Language*.
[15] Ibid., 172.

> *In a minimal cipher,* p *is equivalent to* q*, but only if* p *is considered the token of a type belonging to the expressive plane of a given code a.*[16]

Thus for Eco, cryptography is a special kind of code in which the transposition or substitution of alphabetic letters occurs across the expressive planes according to a set of rules. Using Hjelmslev's sign model, Eco suggests that cryptography is different from natural language because it does not work *across* the semiotic planes. There are two such planes used for natural language (or in the notion of a sign, according to Hjelmslev): the content plane attaches meaning to particular semantic unities (through conceptual or psychological apparatuses), while the expression plane is the material substance of the sign, and is devoid of meaning. Natural language establishes a connection between elements on the expressive plane with elements on the content plane. In working across these semiotic planes, natural language is a system of "double articulation."[17] Cryptography on the other hand, is a system of single articulation, a transcription devoid of meaning, occurring only within the expression plane—from one mark to another mark. For these reasons Eco calls cryptography a correlational code, that is, correlating arbitrary inscriptions.

Eco's definition of cryptography as a correlational code precisely and unambiguously captures the transformational nature of the shift from plaintext to ciphertext. Eco's model helps articulate the way that plaintext (as material substance of the expression plane) is the ground and origin of encryption, and that the semantic violence implicit in cryptography is already part of this original expression. Encryption itself, the transformation from expression plane to expression plane, adds no extra meaning, despite reconfiguring the inscription to make interpretation impossible (that is, interpretation is impossible without first decrypting or cryptanalyzing the ciphertext). However, with Eco's model we are left with something of a sterile characterization, wanting of methods and histories to understand cryptography's various networks and alliances.[18] Kittler offers a less sanitary articulation of cryptography's role in code and code processes.

6.1.2 Friedrich Kittler's definition of code

Kittler defines the transposition of code in terms of media:

[16] Ibid., 173.
[17] Eco, *The Search for the Perfect Language*, 22.
[18] Eco is not, however, unaware of many of these networks and alliances. In his historical work, he has drawn out many connections between cryptography and artificial language planning, as I discussed previously in chapter four. See Eco, *The Search for the Perfect Language*.

> *Given Medium A, organized as a denumerable collection of discrete elements* $E_1^a \ldots E_n^a$*, its transposition into Medium B will consist in reproducing the internal (syntagmatic and paradigmatic) relations between its elements in the collection* $E_1^b \ldots E_m^b$*.*[19]

Compared to Eco's definition, there is a great deal of commonality in his focus on transposition of discrete elements. Kittler envisions a greater role for cryptography than Eco does, believing that in form and origin "codes materialize in processes of encryption."[20] For Kittler, this means that the entirety of the many uses of code in contemporary society—from software[21] to music[22]—are responsible to cryptography. Indeed, there are many ways that code "materializes" in cryptography; Kittler offers four: in communications systems, the vocalic (vowelized) alphabet, mathematics, and language.

According to Kittler, a "developed communications technology" is a "prerequisite for all coding."[23] Kittler argues, probably erroneously,[24] that the Greeks lacked cryptography. According to Kittler, the Romans were the first to put cryptography into wide use, as a consequence of their well developed systems of state communication and bureaucracy.[25] Caesar's cipher (a simple monoalphabetic substitution cipher) developed with, and as a consequence of, the extensive system of Roman diplomatic and military communication. Shortly after Caesar's "invention," Augustus developed the first European "express-mail service" for exclusive use by the military, which by practical necessity required a variety of forms of secrecy, including systems of cryptography.[26] Secrecy was required because, then, as today, mail was subject to search and seizure. The risk of enemy communications intelligence could be alleviated by using trusted messengers who would commit the message to memory (turning the messenger himself into a medium, a point I will return to in chapters seven and eight). But

---

[19] Kittler, *Discourse Networks 1800/1900*, 265.
[20] Kittler, "Code," 40.
[21] Kittler, "There Is No Software"; Kittler, "Protected Mode."
[22] Kittler, *Gramophone, Film, Typewriter*.
[23] Kittler, "Code," 41.
[24] *Pace* Kittler, such codes most likely originated with the concept of writing itself.
[25] This requirement occurs more than once through history. In chapter eight I describe how the Arabs developed cryptanalysis in part as a consequence of their diplomatic, military, and literary traditions. Literary and philosophical translation was an especially important facet of the Muslim caliphates—techniques which were made possible in part due to their well established communications systems. In chapter ten I describe how the Spartans developed the skytale to respond to specific cultural needs for their military communications. The Spartans required a communications system that could ensure messages would not be accidentally uttered—and quite literally uttered, as bad omens would result from the *speaking* of certain words.
[26] Kittler, "Code," 41.

then this solution introduces the possibility of errors resulting from the translation to and from memory, as well as the lack of surety that a messenger is reliable and honest. A wax seal to enclose an envelope could be used to provide authentication and integrity (ensuring that the message received was sent from the indicated person, and had not been tampered with), but for secrecy, cryptography outperformed a sealed envelope.

With the onset of modernity, this requirement for secret message transmission became more acute: the letter transformed into the postcard, and in turn became the telegraph or the teletype—a process Siegert describes as the transformation of literature into code. As postcards developed, the shift away from interpretation, towards code, resulted in a further economization of communication. Due to rules placed on postcard postage materials and rates (the sender could make only minimal marks to a preprinted card), various forms of "Universal Correspondence Cards" were invented, which further transformed language,[27] presenting language itself as a set of stock phrases. (Specifically, the sender marks selected boxes to construct a combinatory message, or writes single words in predetermined spaces, *Mad Libs*-style). This mode of communication was promoted as a rhetorical goal, turning the everyman into Tacitus, an ideal of brevity.[28] Codes for telegrams, structurally similar to encryption, also required brevity.[29] And then in the computer era, code proliferated to ubiquity.

This transformation towards computer code ushered in new ways of reading and writing. Kittler pointed out that the word "code" originally related to codex, and came to be synonymous with a bound book of laws. Stabilized in a codex, according to Kittler, message transmission transformed into data storage, as a symptom of the ways code turns "pure events into serial order."[30] That is, the "events" of speech—each word dutifully following the former—were transformed into the two-dimensional, visual plane of the codex, enabling rapid lookup and reference across the page. The codex itself then transformed back into a one-dimensional (but higher-order) plane of code. Thus serialized in computer code, the time-axis of each predecessor—speech and the codex—could be further manipulated,[31] with the human lifeworld represented as strings of data to be edited, concatenated, stored, and searched.

---

[27] Siegert, *Relays*, 156.
[28] Ibid., 150.
[29] Kittler derives the same conclusion but uses the development of the typewriter as his premise, instead of the postcard. See Kittler, *Gramophone, Film, Typewriter*.
[30] Kittler, "Code," 41.
[31] Krämer, "The Cultural Techniques of Time Axis Manipulation."

Although we typically associate code with computer technology or genetic bio-engineering, Kittler pointed out that while codes only gained *prominence* during an age of high technology, they are in fact the result of much older technologies. The origins of code are found in the development of "true alphabets, as opposed to mere ideograms or logograms."[32] Kittler remarked that the vocalic (vowelized) alphabet of the Greeks was a necessary but not sufficient condition for code, and that in fact alphabets were the prototype for everything discrete for the first three and a half millennia.[33] For most of these three and a half millennia, "code" meant written words that were pronounceable (due to the vowels added by the Greeks), but with the introduction of ciphers, a bifurcation occurred. Although Kittler failed to recognize it, the introduction of ciphers made code unpronounceable, that is, silent.[34] On Kittler's timeline, ciphers were made possible by the Greeks, introduced with the Romans, and developed significantly with Alberti's invention of polyalphabetic encryption.

Kittler argued that Alberti's invention of polyalphabetic encryption ushered in a new discursive regime.[35] Alberti was aware that letter frequencies were the key to cryptanalysis of old Caesar-type (monoalpabetic) ciphers, and that his polyalphabetic encryption defeated these simple forms of cryptanalysis. The critical development were tables of letter frequencies that in the West were made possible by the analytic work of printers, who had a practical necessity to count letter frequencies in natural languages so as to ensure sufficient metal type was on hand for print jobs.[36] It is because of this dependency on letter frequency analysis that Kittler concludes, "without Gutenberg's printing press… [there would be]… no cryptology." Much later, this same process would be repeated by Morse, who used the printers' letter frequency tabulations to optimize his telegraph codes.

It was a century after Alberti and Gutenberg when, according to Kittler, the seminal moment came for code and cryptography. The French mathematician François Viète developed a notion of "unknowns and universal coefficients written with numbers encoded as letters" as a necessary conceptual breakthrough for his invention of modern algebra.[37] The important conceptual

[32] Kittler, "Code," 44. See also the discussion in chapter three.
[33] Ibid. In chapter five I argue against Kittler's interpretation that the introduction of vowels was essential.
[34] See chapter eleven for a discussion of silence and cryptography.
[35] See chapter three for a description of Alberti's *De Cifris*.
[36] See chapter nine for a further discussion of the role of letter frequency analysis for cryptanalysis.
[37] Kittler, "Code," 42.

move was to invent a new character, what Viète called "*logistica speciosa*," a mathematics of species, rather than individual, definite numbers.[38] The basic concepts of Viète's algebra paralleled those techniques he developed for codebreaking. And in fact, given that Viète's primary occupation was as a royal counselor,[39] which required skill in code breaking, it is fair to say that these conceptual advances were for, in the first instance, cryptology, and only in a more academic sense, for mathematics. Although Viète was not the first to align cryptography and mathematics (the Arabs did this half a millennium earlier),[40] in the West, the tie that Viète bound would not loosen. When Turing later published his work on computable numbers (in 1936), as the analytical predecessor and conceptual requirement to the construction of the Allied codebreaking machine Colossus, mathematics and encryption "entered that inseparable union," Kittler wrote, "that rules our lives."[41]

Kittler also regarded code's relationship to language as an insoluble dilemma.[42] The cryptanalytic and storage capacities of the NSA accelerated the computer age by sacrificing literature, according to Kittler, since only those words that are processed become *real* (in the Lacanian sense of emerging outside of language in the process of signification). Kittler opined "we do not write anymore" because we only "wordprocess a text."[43] In fact, the "last historical act of writing" occurred in the early 1970s when computer engineers working at Intel rolled out a large sheet of paper to manually lay out the circuitry of the 8086 computer chip. In Kittler's mind, by constructing the 8086 chip, the engineers developed a new word-processing machine capable of severing the relationship between the hand and literature which had previously existed in the discourse network 1900.

In the following case study, I attempt to apply the insights gained from Eco and Kittler's analysis of code and its intersection with cryptography. Such an investigation of code will look a lot like the emerging fields of software studies and critical code studies (a field that Kittler influenced deeply). This is no excursion, however, since one of my implicit goals in studying cryptography has been to show that, if in a preliminary and tentative way, cryptography is a legitimate topic of study for these fields which have not "historically 'owned' software," as Fuller offers in his exposition of the key criteria of software

[38] Pesic, "Secrets, Symbols, and Systems," 677.
[39] Ibid., 675.
[40] See chapter nine for the history of cryptanalysis and the role of Arab statistics.
[41] Kittler, "Code," 43. See also Mackenzie, "Undecidability"; Dyson, *Turing's Cathedral*.
[42] Kittler, "Code," 46.
[43] Ibid.

studies. Like Eco and Kittler, Fuller's definition of software studies recognizes that such a study must attend to the materialities of software, the working of computation (in the face of too much study of communication crossing an information channel), and the multiplicity of scale (we often think of code as "micro" and ever shrinking, but massive computing systems now behave like large-scale infrastructure instead). In the example that follows, the configurations of code depend crucially on these kinds of questions, even though the subject of the case study is small, boutique, and artsy.[44]

6.2 Agrippa (A book of the dead)

In 1992, cyberpunk author William Gibson was commissioned to write a short poem to be included in a noir art book published by Kevin Begos, Jr. and designed by Dennis Ashbaugh. The result was *Agrippa (A Book of the Dead)*. This lavishly decorated book contains copperplate aquatint etching of simulated DNA gel electrophoresis, long DNA sequences from the bicoid morphogen gene of the fruitfly, and a number of faded, vintage, advertisements (the book was published in two versions, the so-called "small" version being less elaborate than the "deluxe" version).[45] These material furnishings portray the ubiquity of codes—the way they come into being, and how they are forgotten. Additionally, a 3.5" diskette was embedded in the back of the book. This diskette contained a Mac System 7 program that, when run, scrolled Gibson's poem on screen. The poem could be viewed only a single time, which would then self-destruct (supposedly using an "encryption" algorithm, although, as I discuss below, this is not quite right). The poem, in keeping with the motif of the book, tells about memory, loss, nature, and mechanism, all framed by a Kodak photo album.

When released in 1992 the poem attracted considerable attention, but due to the extremely limited production run very few people have seen the book or the poem first-hand. In an interesting twist of fate, a transcript and then a video recording of the poem surfaced online.[46] These early leaks (surreptitiously recorded) came from a public showing of the software, known as the "The Transmission," held in The Kitchen, an art space in New York City. For over a decade this was the only source of information about *Agrippa*. Then in 2005,

[44] *Agrippa* has often been seen as participating in a New Aesthetic, and is a primary artifact for new kinds of Digital Humanities. See Jones, *The Emergence of the Digital Humanities*, 79, who follows up on my initial research on Agrippa.
[45] Liu et al., "The Agrippa Files."
[46] Kirschenbaum, *Mechanisms*.

Alan Liu and a team of graduate students created the scholarly site, *The Agrippa Files*, working in collaboration with Matthew Kirschenbaum at the *Maryland Institute for Technology* in the Humanities and the Digital Forensics Lab.[47] *The Agrippa Files* site contains numerous archival documents detailing the production of *Agrippa,* including a bit-for-bit copy of the *Agrippa* application, archived from a disk loaned to the team (in 2007) by *Agrippa* collector Allan Chasanoff.[48] The disk archival process was performed by a team at the University of Maryland, lead by Kirschenbaum. The Maryland team was successful in duplicating the original disk (without damaging it, or triggering any viruses, as was a worry),[49] and then they were able to run the Mac OS 7 application in a software emulator.[50] For the first time since "The Transmission," the *Agrippa* code was executed.

The success of the archive and emulation of *Agrippa* offered the team "a kind of closure," because the "mechanisms are now known and documented."[51] This conclusion was too hasty, however, and the team knew it. They wrote,

> *Indeed, there are at least two primal artifacts that remain beyond reach. The first is the source code for the encryption program, a few scraps of which survive in hard copy and are viewable amongst the materials on The Agrippa Files site. The second is the electronic manuscript of the poem itself, marooned on whatever computer Gibson originally wrote it on, wherever that machine is now (if it even still exists as functional hardware).*[52]

Following this lead, I knew that the true *Agrippa* remained out of reach because the mysterious cryptographic routines it contained were still unexplored, and these critically bound the entire work together.

---

[47] Ibid., 245 ff.
[48] Liu et al., "The Agrippa Files."
[49] A second disk included in the Agrippa book was not successfully duplicated. This second disk is not of the same brand or format as the application disk, and has been spray-painted black, presumably for use as a prop. The inability to duplicate, let alone run this second disk, offers further tantalizing possibilities. Just as the early *Agrippa* scholars took it on faith that the *Agrippa* application ran as advertised, but later realized this assumption was false, we can likewise question the assumption that this second disk is merely a prop. Even if the second disk does not contain a runnable application, what accidental, hidden, or vestigial code might it contain?
[50] Kirschenbaum, Liu, and Reside, "No Round Trip."
[51] Ibid.
[52] Ibid.

Twenty years after its initial release, I held a code breaking contest to crack *Agrippa*, using the collected materials made possible by *The Agrippa Files* site.[53] The details revealed during the contest turned existing scholarship on *Agrippa* upside down. *Agrippa* deceived everyone—lying about its operations, and tricking early scholars into believing that the case had been solved. (We might still ask, what tricks and deceits are left today?) Later reflecting on the results of the contest I launched, Liu offered a mea culpa on his own and other's early research, suggesting that *Agrippa* was too mysterious and enticing to wait for further forensics. Riffing on what McGann calls "romantic ideology" (the implicit identification of professional scholars with the ethos of the very writers they study), Liu admits that the initial *Agrippa* scholars had "been apologists of *neuromantic* ideology."[54] The supposed self-encryption function that was the key feature of the *Agrippa* application, which so enticed, would eventually break it all open—living up to its viral claim and "just waiting to break free of the confines of an art book to go feral" as Liu puts it.[55] Indeed, *Agrippa's* domestication inside *The Agrippa Files* archive was short lived.

The following forensic description of *Agrippa* is the result of an online cracking challenge that I created to marshal the expertise needed to crack *Agrippa* (full details of the contest were published elsewhere).[56] The result of this contest was that *Agrippa* was successfully reverse-engineered and tools were implemented to extract the ciphertext, crack it, and display the original plaintext. This original contest and the results (including an interactive encryption/decryption tool) are hosted online at http://crackingagrippa.net.

6.2.1 Forensic description of Agrippa

When *Agrippa* was first published there was considerable ambiguity about the poem's "mechanism," which only permitted viewing the poem a single time. Some had suggested that it was a destructive virus, or that it triggered automatically when the disk was inserted into a computer. When Liu and Kirschenbaum began their forensic investigation of the software, they discovered that it was relatively easy to make a bit-for-bit copy of the loaned

[53] As with all scholarship, but especially so with technical artifacts like *Agrippa*, without the hard work and tangible results of early *Agrippa* scholarship, the code-breaking contest would have been impossible, and *Agrippa's* inner workings would have remained secret and inaccessible. I would like to personally extend my sincerest thanks to Alan Liu and Matthew Kirschenbaum who proved invaluable before, during, and after this research.
[54] Liu, "Commentary by Alan Liu."
[55] Ibid.
[56] Portions of this chapter were published previously, see DuPont, "Cracking the Agrippa Code: Creativity Without Destruction."

disk using modern tools (Linux's dd tool). While no virus or automatic triggering was found, the team discovered that, as anticipated, the program would in fact run only a single time. Of course, with a digital copy from the pristine original disk, infinite copies could be made. From each new digital copy the application could be run time and time again, simply throwing away the "destroyed" version after each run.

Based on information in the archival documents, Liu and Kirschenbaum assumed that the "self-destruct" mechanism was a (re-)encryption of the poem. Liu had used *Agrippa's* self-destruct mechanism as an "exhibit" of his thesis of "destructive creativity," in large part because he believed the cryptographic mechanism in *Agrippa* erased the poem once it displayed (as it was advertised to do). Liu's thesis of "destructive creativity" reversed Schumpeter's dictum (creative destruction), exposing how destruction "*becomes* creativity" (emphasis in original)—that is, *Agrippa* exhibits an "alternate creativity."[57] Liu points out that *Agrippa's* creativity is "heretic" because it is attributed to an automatic mechanism rather than natural intellect and inspiration, as is typically the case with conventional art and craft.

Kirschenbaum had used *Agrippa* to make a point about never being able to recapture the original context of the artifact, despite the many layers and sedimentation that had been added in the years since its inception. On account of this necessary arrow of time, and the technical slippage between what Kirschenbaum calls "forensic" and "formal" materiality,[58] he argued that there was no "round-trip" for *Agrippa*. The impossibility of a "round-trip" also holds a certain kind of logic in the framing of the supposed self-destruct encryption mechanism. If *Agrippa* had lived up to its goal of self-destruction, there would have in fact been no "round trip," at least by typical means. Kirschenbaum's work highlights the fact that even when the materialities of digital objects have been compromised, a certain amount of the "original" information is usually still present (as in the example of the destroyed hard drive from the World Trade Center, from the cover of his book *Mechanisms,* which forensics experts were still able to recover information from). Similarly, the formal properties of digital objects are extremely durable (so long as the effort is made to maintain them), yet very brittle, as they might exist forever but become meaningless very quickly if the systems and contexts they are embedded in change.

The results of the codebreaking contest prima facie problematized Liu and Kirchenbaum's theses. Neither author had paid too much attention to the fact

[57] Liu, *The Laws of Cool*, 340.
[58] Kirschenbaum, *Mechanisms*, 10–11.

that *Agrippa's* self-destruct mechanism was supposed to be cryptographic, as had been claimed in the marketing material (as we will see below, this turned out to be false, but in an interesting way). If *Agrippa* really was cryptographic, it would mean that for Liu's interpretation of *Agrippa*, his thesis of destructive creativity, is hollow, since nothing is destroyed. With the correct key (or through cryptanalysis), the "original" was always potentially available, and indeed, then, nothing was new (but, recall the sense of violence that occurs from the very act of calling something plaintext, or encryption it—even if the original is obtained by decryption, as I discuss in chapter five). This conclusion taps into the essence of cryptography—as a category of expression, in order to have meaning distinct from mimetic forms of writing, cryptography must exclude erasure and destruction, even "creative" destructivity. And for Kirschenbaum's interpretation of *Agrippa*, we might imagine that the whole point of ostensibly using cryptography was to realize the *potential* for a round trip. The essential point of cryptography is to enable a return, or round trip, as a type of remembrance. In fact, the poem's central motif and mechanism is the Kodak album—as pure of a memory device as we have, evoking the ways that cryptography has been part of memory traditions from the earliest days (recall the discussion of memory in the systems of representation from chapter three). Yet, *Agrippa* failed to live up to its cryptographic boasts, and in a way, *Agrippa* ends up *vindicating* Liu and Kirschenbaum's theses.

Agrippa is not destroyed when run—it can still be either decrypted or cryptanalysed—although a particular kind of self-destruction does occur. This strange self-destruction leaves the ciphertext untouched, but forcefully erases critical components of the executable binary.[59] Running the application does result in a kind of digital *auto-da-fé*, as Liu originally thought.[60] And both the encryption and the (separate) self-destruct mechanism do contribute vitally to the aesthetic performance of *Agrippa.* Critically, the results of the contest also proved that cryptography is central to the mechanism and its artistic performance, but not as part of its self-destruction.

Before I launched the codebreaking contest I attempted to crack *Agrippa* myself. But, even though the cryptographic algorithm turned out to be very insecure, even for its release in 1992, I quickly discovered that cracking *Agrippa* was a considerable technical challenge. Of course, without the prior efforts of

[59] The software program is made up of "code," of the sort that most people are familiar with, but the code must be compiled in order to be executable on a computer. The result is a file made up of computer-executable instructions, called a "binary" (even though all files on the computer are technically encoded in binary).

[60] Liu, *The Laws of Cool.*

The Agrippa Files, cracking *Agrippa* would have been a non-starter, since the obscurity of physical copies meant that there was no readily available binary before their archival work. Even with the archival documents and the binary, however, after several weeks attempting cryptanalysis, I realized that I would need to enlist outside help.

I decided that I would marshal help by creating an online "cracking" or code-breaking challenge. Cracking challenges are relatively common in some subcultures on the Web, but this one was complicated by the fact that *Agrippa* had been developed 20 years prior and seemed to follow very few industry practices. Cracking *Agrippa* requires knowledge of 1992-era Macintosh software development processes, tools, and languages. And, once the software yields the ciphertext, the would-be cracker must possess skills of cryptanalysis.

When I launched the contest the immediate interest was considerable—quickly breaking out of its confines as an academic project and garnering interest in mainstream and general technology news. Within hours I was made aware of at least a few serious attempts to crack the code, and in just a few days the first contest submission was filed. Hours after the first submission I received several others, and after confirming the success of the first submission I closed the contest. After carefully working through the submissions with the contestants (who provided the substance of this forensic account), I discovered that there are four main aspects to the *Agrippa* program: the compiled binary, the main cryptographic algorithm, the encryption effect that runs after the poem finishes scrolling, and the self-destruct mechanism that prohibits running the program more than once.

6.2.1.1 The compiled binary

The *Agrippa* program was developed using Macintosh Allegro Common Lisp, possibly version 1.2.2 or 1.2.3, and bundled as a self-extracting binary. As mentioned in *The Agrippa Files* archival documents, the initial plan for an auto-run, virus mechanism was never developed,[61] and while there are some tricks to impede reverse-engineering the program, the programmer's boasts that it would be impossible to run through a debugger are unfounded. The Macintosh Lisp compiler uses Lempel–Ziv–Welch (LZW) compression, with the poem stored as encrypted text in a string variable ("zi") (one contest submission suggested that variable names may correspond to non-English words, in this case, "zi" means "words" in Chinese). This variable is encoded in the MacRoman character set, but only uses ASCII characters (low in the MacRoman table), so

[61] Liu et al., "The Agrippa Files."

the visible effect is indistinguishable from ASCII. Offset values were discovered for most aspects of the *Agrippa* binary.[62]

As was known in 1992, and exploited by a number of the contestants, Macintosh Lisp contains an error (not binding a keyboard handler at a particular point) that allows one to drop out of the program and into a Lisp Run-Eval-Print-Loop (REPL) console. With access to the REPL, arbitrary code may be run and interaction with the variables and routines reveals much of the source contents (however, the REPL is of limited utility because many variables are uninitialized, so constants are incorrect). By exploiting this error, it was discovered that the shipped production code does not exactly match the archived (partial) source code printout from *The Agrippa Files*. This suggests that the archival document was from an earlier stage of development. Several routines either changed names or no longer exist, e.g., UN-WAYMUTE-IT, UN-PERMUTE-IT, and UN-ROLL-THE-TEXT (which is thought to correspond to UN-ROLL-ZI).

6.2.1.2 The cryptographic algorithm

The *Agrippa* poem is pre-encrypted and stored as a string variable in the program. The ciphertext is not visible in the binary due to the LZW compression. All contestants discovered that the cryptographic algorithm is a custom RSA function that encrypts in three-character blocks, with additional "bit-scrambling" permutations (a kind of simple substitution cipher). Because the poem comes pre-encrypted, there is no encryption routine in the program: the program simply loads the ciphertext, decrypts it to memory, and then abandons the plaintext (still in memory). As proof of this, the same decryption routine can work on a "fresh" disk as well as previously-run "corrupted" disk (more on the "corruption" below); two contestants implemented a tool to decrypt from the compiled binary in either state (requiring reverse-engineering of the LZW compression, which was at least as difficult as cryptanalyzing the weak cipher, highlighting the parallels between "code" and cryptography).

[62] These are available at the contest website: http://www.crackingagrippa.net.

The cryptography is applied identically and independently to three-character blocks (resulting in cryptographic weaknesses, see below). On each block the cryptographic routine performs three distinct steps: first a bit permutation (substitution cipher) that converts three 8-bit characters into two 12-bit characters, then an RSA transformation using a 12-bit key, and finally another bit permutation that converts the two 12-bit characters back into three 8-bit characters (corresponding to ASCII-encoded text) (see figure 6.1).

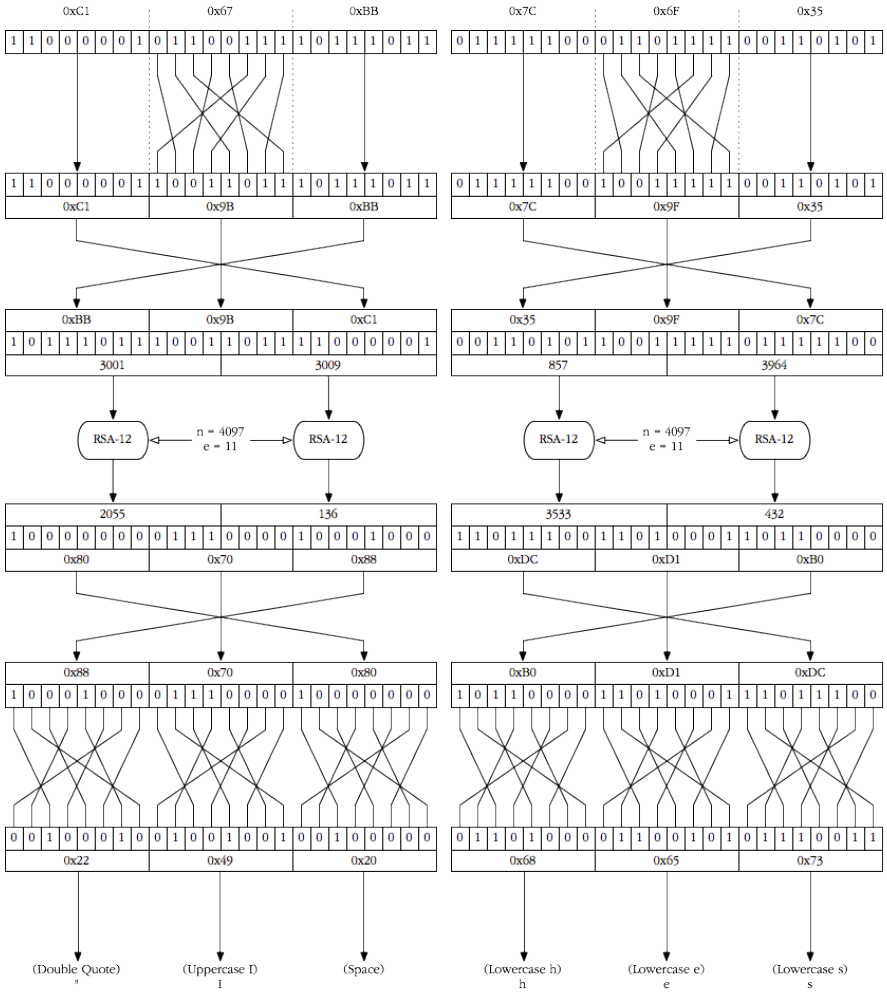


Figure 6.1: Contestant Jeremy Cooper's graphical depiction of the decryption process.[63]

The RSA cryptography has a public modulus of 4,097 (from primes 17 x 241), and a public exponent of 11. Due to the extremely short bit-length of the public

[63] Licensed under Creative Commons Attribution-Non Commercial 3.0 Unported License. DuPont, "Cracking the Agrippa Code."

modulus and exponent, the private exponent can be found easily (either through brute-force or the Chinese Remainder Theorem), and was revealed to be 3,491 (the private modulus is always the same as the public modulus, 4,097). So, the RSA encryption process is to take some number *x* to the 3491st power, modulus 4,097—however, recall, the encryption routine is not present in *Agrippa*, and was therefore reverse-engineered once the private exponent was discovered.

Evidently, the anonymous *Agrippa* programmer was either undecided or confused about what kind of encryption to employ, remarking in a letter that the cryptography would be similar to both Data Encryption Standard (DES) and RSA (the prior being a symmetrical key cryptography algorithm, and the latter asymmetrical): "another info source would be anything on the Data Encryption standard or mathematical works by Rivest, Shanker [*sic*], Aldemann [*sic*]."[64] Likewise, the cryptographic routines are named with references to DES, even though they are RSA.

The anonymous programmer attempted to strengthen the cryptography by using a more sophisticated mechanism for block enciphering (where the same key is re-used for each block, but ideally "mixed" with the neighboring block); the programmer remarked, "The value, both character and numerical, of any particular character is determined by the characters next to it, which from a cryptoanalysis [*sic*] or code-breaking point of view is an utter nightmare."[65] Yet, in reality the encryption is applied identically to each three-character block, in a mode of operation known as Electronic Codebook (ECB). This simple mode of operation has many cryptographic weaknesses, most visibly the fact that identical blocks will encrypt to the same result. For example, in the plaintext of the poem, there are numerous sections of three consecutive spaces which encrypt to "space, e with circumflex, backslash," or in decimal 20 136 92 (with quotes added for clarity, displayed as ASCII: " ê\"). Even without reverse-engineering the algorithm, this weakness is significant and exposes the ciphertext to old-fashioned statistical analysis (where trigrams would be visible in the ciphertext). Similarly, the three-character block size and ECB mode of operation explain the curious two spaces at the end of the poem.[66] Rather than signaling the end of the poem as Wiedijk (an early *Agrippa* scholar) thought, the two spaces at the end of the poem are needed to pad the block, otherwise the cryptographic routine would fail.

[64] Anonymous, "Letter from Programmer (Item #D6) (Transcription)."
[65] Ibid.
[66] Wiedijk, "Original Text of Gibson's 'Agrippa' Poem Extracted From Disk."

When *Agrippa* was released in 1992, the United States famously classified all cryptographic materials as munitions and restricted the export of "strong" cryptography.[67] *Agrippa* was seen by cypherpunks and computer scientists as a challenge to these stifling and backwards cryptography export controls. Yet, given the extremely short key-length (12 bits), *Agrippa* would never have been prevented from export—in 1992 the United States permitted an RSA key of 512 bits. Indeed, the political involvement of John Perry Barlow and the Electronic Frontier Foundation was superfluous given that *Agrippa* would not have been considered strong cryptography.[68]

6.2.1.3 Encryption effect

When *Agrippa* is run, the poem slowly scrolls down the screen, and once the poem has finished scrolling, it displays an encryption effect; seemingly to evoke the idea that the poem is re-encrypted. Once the encryption effect has run, the poem will not display again. As discussed above, there is no RSA encryption algorithm in the binary, however, by running the plaintext through a permutation routine (re-purposed from the main *de*cryption algorithm), the plaintext is effectively encrypted using a simple substitution cipher. While this is a re-encryption of the plaintext, it is actually only for visual effect since the ciphertext generated by the substitution cipher is not saved back to disk, but is instead displayed and then abandoned. Once *Agrippa* is run, only one change is saved to disk: the "self-destruct" mechanism.

6.2.1.4 The "self-destruct" mechanism

Agrippa famously runs only a single time. There are a number of possible mechanisms to cause a self-modifying program to run only once. For example, one could flip a switch in the binary that alerts the main routine that the program has previously been run, or re-encrypt the data and throw the key away (possibly generated dynamically with runtime variables), and so on. The anonymous programmer of *Agrippa* chose a simple mechanism: write a large string of data over a portion of the binary that contains necessary runtime routines. In the archived source code printout, this self-destruct mechanism wrote 40,000 ASCII characters (ASCII code 255) to a specified offset, leaving a string of 320,000 binary 1s to corrupt the program. Evidently, at some later stage of development, someone thought it would be more in keeping with the theme to write a fake genetic sequence (CTAG's) instead of merely 1s.

[67] Diffie and Landau, "The Export of Cryptography in the 20th and the 21st Centuries."
[68] Barlow, "Letter from John Perry Barlow to Kevin Begos (Item #D45) (Transcription)."

This self-destruct routine is called MAKE-SOME-SHIT, and is located in the archival source code listing halfway across page three and the missing page four. It was revealed that MAKE-SOME-SHIT uses a fixed seed to call the Mac Toolbox Random Number Generator, which saves 6,000 characters (either C, T, A, or G) to the disk (at offset 680168). While the offset chosen for self-destruction does effectively corrupt the program, it does not destroy the ciphertext. Two cryptanalysis implementations (available on the contest website) can decrypt the poem from either a "fresh" or corrupted binary, since the self-destruct mechanism left the ciphertext intact.

One contestant speculated that page four of the source code listing might have been omitted from the *Agrippa Files* archive due to the presence of the word "SHIT" in the routine name. Liu later took this routine's name as an emblem for *Agrippa's* ability to continue to generate interest and vex attempts to fully understand the artifact. It turned out that the mechanism that mattered most was called MAKE-SOME-SHIT—not some fancy cryptography. It vulgarly printed out fake codes to obliterate the executable binary. So, it isn't so much that *Agrippa* lied, or proved Liu and Kirschenbaum's earlier theses wrong, rather, *Agrippa* simply made some shit.

❦

Cracking the *Agrippa* code was yet another performance of this fascinating artifact. I showed that while Liu's argument about the "destructive creativity" of *Agrippa's* encryption is in a way hollow, something of equal fascination has taken its place. Perhaps shit and destruction are social products more closely aligned than we like to think—in our age of humanitarian and climate crisis? Additionally, Kirschenbaum's argument that there is "no round trip" does not hold for *Agrippa's* cryptography, since by necessity plaintext must always be potentially available for recovery. But, to learn from Kirschenbaum's exploration of digital mechanisms, the gap between real and potential—material and formal—also matters immensely for *Agrippa's* cryptography. That plaintext is always a potential outcome of decryption or cryptanalysis of ciphertext is not the same thing as *choosing* to write 'in the clear.' The conclusion that we should deploy cryptography universally only makes sense given the premise that encryption is always reversible, on the most instrumental of accounts. Recovering old codes, even with relatively simple examples like *Agrippa*, is no easy matter. And more importantly, as I explore in chapter twelve, a politics of cryptography capable of moving beyond the binaries of strong encryption or wholesale surveillance needs to understand that visibility is contextual, embedded, and necessarily contested.

7
Cryptographic media

When plaintext is encrypted, it reconfigures our relationship to notation. We should recognize that, in a conventional sense, encryption is said to be an algorithmic process that generates secrecy in the conversion of plaintext into ciphertext. This process, interrogated in the discussion of plaintext in part one of the present work, need not require mathematics or the invocation of numbers, but it does often make use of some mathematics to ensure tractable secrecy (as we have seen, this has been especially true for the development of cryptography over the last century). On my analysis, however, encryption is an algorithmic process that performs conversion *in situ*—the machine (paper and pencil, cipher wheel, electric computer, quantum computer, and so on) manipulates notational inscriptions by applying a deterministic process which outputs a corresponding ciphertext. In this process, the algorithm provides an active kind of "sending" (without movement), as a vector—from readable plaintext to unreadable ciphertext. The corresponding ciphertext is typically a high entropy reordering of the original plaintext, such that the semiotic or representational link to the original message is practically severed (it cannot be "read" without first being decrypted or cryptanalysed).[1]

The resulting ciphertext is a type of media and may simply be stored—the sheets of paper filed away, or the memory addresses written to disk—or more typically, encryption is a mediatic part of an active communication process. Encryption, however, does not provide the communication mechanism itself—that is left up to the postal service, the email protocol, and so on—but encryption enables the communication of messages without a physical barrier or enclosure.[2] In this way, an encrypted postcard is like a letter in a closed envelope—and if the postcard also contains a hash signature, it is like a closed envelope with a special wax seal used to authenticate the sender. So, while communication is not a necessary component of encryption, it is a common and powerful part.

But algorithms and communications protocols do not tell the whole story. Across the next three chapters, I investigate how media become central problematics for encryption. In this short chapter, I introduce the theme of

[1] See chapter ten for a discussion of entropy and order in ciphertext.
[2] See the discussion of postal services, envelopes, and postcards in chapter six.

cryptographic media by investigating the ways that encryption stands between plaintext and ciphertext. I describe one way that cryptographers have historically aspired to intensify the powers of encryption. In this curious history, cryptographers have attempted to close the medial gap of communication by transforming encryption into perception, by making the distant a feature of the local. To demonstrate this point, I investigate the cryptographically-curious author, Edgar Allan Poe, and his spiritual followers, who attempted to turn transmissive (that is, primarily temporal) encryption into communicative (primarily spatial) encryption. One way this reconfiguration of cryptography was attempted is through "telepathic" forms of encryption, where perception across vast distance would require an impossible medium and method, a feature that was often considered an plausible upper limit (and goal) for truly powerful encryption. This discussion of cryptographic media sets up the following chapters.

In chapter eight, I investigate a messenger model of encryption in the form of transmission across media. The messenger model has two different modes, roughly paralleling the instrumentalist formulation: 1) the use of encryption for communication 2) the use of encryption for algorithmic processing, as transmission *in situ* (this special sense of "transmission" comes from Regis Debray, who distinguishes its stationary mode of operation from communication). The metaphor of messengers is also found in the myth of angels, media *par excellence*. Hermes is the trickster messenger angel of communication,[3] and Iris is the iridescent angel of *in situ* transmission and vectors. Correspondingly, Hermes' media action is "communication" and Iris' media actions is "transmission."

In chapter nine, I return to the history of cryptography and language introduced in chapter four, this time drawing a distinction between cryptographic encryption and linguistic translation as forms of media. Previously, I described how cryptography was deeply related to universal and perfect languages, which, by the end of the eighteenth century, was no longer a reality. After the discourse networks of 1800 and 1900, insipient instrumentalization blossomed through the late twentieth century. After the Second World War, cryptography became a field of study within electrical engineering and eventually, computer science. During this process, encryption

[3] Hermes is not always conflated with angels, which are of a Christian tradition, but in the Homeric hymn to Hestia, Hermes is called *angelos*, which means "messenger" and gives us our word for angel. Similarly, Mercury is the Roman name for Hermes in his capacity as a merchant, with "merchant" and "Mercury" sharing the same etymological root. See Galloway, "Love in the Middle," 31.

played a role in the theorization and practical development of language translation. As a medium between two languages, however, I note that encryption and decryption can only ever be a process of transcription, and in that chapter, I discuss how cryptanalysis gestures towards true translation (not transcription). Correspondingly, cryptanalysis fails to maintain the formal identities required for notational representation (as discussed in chapter five).

7.1 THE PRIMAL SCENE OF CRYPTOGRAPHY

For each of the chapters, encryption stands "between" plaintext and ciphertext. As a "between," encryption is a medium. Kittler discovered the historical linkage of "between" and "medium" while reading one of McLuhan's letters about how Aristotle's form and matter ontology excluded questions of media. According to Kittler, if we were to only read the *Metaphysics* we would agree with McLuhan's assessment, that, because of Aristotle's influence, "our philosophy systematically excludes techné from its meditations."[4] In the *Metaphysics,* McLuhan noted, Aristotle dealt only with "things, their matter and form" but not the "relations between things in time and space," which excluded the technical relations of media.[5] What McLuhan missed, Kittler pointed out, is that Aristotle *does* discuss the question of media—but only in his psychological work *De Anima*.

Aristotle's original use of the term "medium" was strategically linked to the medium of *perception*. The questions facing Aristotle were: how can the eye view a remote object, and how can the ear hear a distant sound? Was the medium *between* (*metaxú*) the object and the organ of sense perception a vacuum (that is, nothing), as some of his atomistic predecessors believed? Or was the medium some kind of transparent (or "diaphanous") material that enabled the remote object to "touch" the sense organ?

Perception, according to Aristotle, must presuppose a physical medium, but transparency is a functional necessity, on account of being an intervening medium. That is, the medium must not show itself, or in Krämer's discussion of Aristotle's media theory: the medium is "a manifestation only when it does not manifest itself".[6] Similarly, Ernst argues, the in-between does not manipulate the signal, instead it makes itself apparently disappear, like the disappearance of

[4] McLuhan "Letters" quoted in Kittler, "Towards an Ontology of Media," 25.
[5] Ibid., 24.
[6] Krämer, *Medium, Messenger, Transmission*, 32.

the translator.[7] For Aristotle, perception has two functions: "Aristotle talks of sensual perception," Weber writes, and thus "the medium becomes a condition not only of contact, but also of *transmission*."[8] The result of Aristotle's philosophical treatment of perception was that the common Greek preposition "between" (*metaxú*) was converted into the philosophical concept of "media," *tò metaxú*.[9]

To contrast this view of cryptography with the typical instrumentalist account, consider the way that the algorithms and processes in the "middle" of encryption are vitally important for understanding how cryptography works. These processes determine security, and demarcate between the various types of cryptography (e.g., AES encryption is different from DES encryption precisely because of these middle processes). For the mediatic account, the encrypting "middle" is what Krämer calls the "primal scene of media."[10] For Krämer, the primal scene of media is occupied by two views of the philosophy of media, a technical/postal media philosophy (roughly equivalent to the technical model of communication put forth by Shannon and Weaver),[11] and an "erotic" media philosophy. The "erotic" form presupposes that communication is symmetrical and reciprocal, with the goal of unification and symmetrical (dialogical) communication. The technical/postal view of media is based on the notion that all communication requires an intervening medium, yet communication is only successful when this medium fades into the background and remains unobtrusive. Both models have certain alliances with a mediatic conception of cryptography.

According to Krämer, the "erotic" model of media, associated with the views of Jürgen Habermas, uses dialogue to collapse distance and unify the subject and object (unified, on account of being erotic, by the proximity of sense organ copulation). This model requires, in the first instance, human subjects in reciprocal interaction. Since distance stymies the coordination of dialogue, its ideal presupposes the "death of distance." This is also a feature of technical communication, since successful communication is achieved by eliminating mediating apparatuses to the greatest extent possible. Furthermore, as will be discussed in chapter ten, for cryptography, the alterity of ciphertext actively mitigates against any unification of source and destination "distance."

---

[7] Ernst, *Digital Memory and the Archive*, 105. See also chapter nine for a full discussion of translation.
[8] Weber quoted in Ibid.
[9] Kittler, "Towards an Ontology of Media," 26.
[10] Krämer, *Medium, Messenger, Transmission*, 25.
[11] Weaver, "Recent Contributions to the Mathematical Theory of Communication."

The technical/postal model, on the other hand, enlists the capacities of a messenger to bridge but not annihilate distance, which is a significant conceptual advantage when discussing cryptographic media. The messenger bridges the distance between the remote Other of ciphertext and the proximate, intelligible plaintext through processes of encryption/decryption (and cryptanalysis).[12] Therefore, the distance or alterity is crossed, rather than eliminated. Krämer enlists the messenger as a key metaphor for all medial processes. The messenger is a useful metaphor because it bridges the divide or difference between heteronomous worlds,[13] but also preserves the distance that separates them.[14] Krämer's messenger model is directed against hermeneutics, (even though Hermes is the figure of the messenger—the word "hermeneutics" is from "Hermes"). The messenger model points towards a subject-free theory of communication that challenges the notion of media that works through autonomous agents, and those which result from cultural and historical dynamics (such as Kittler's famous dictum that "media determine our situation").[15] Instead, it is precisely the invisibility of the messenger that enables it to function as a transmitter to be easily replaced by non-human or technical entities.

The messenger metaphor is part of the transmission model of the postal principle, and the transmission model excludes the communicative model. The communicative model presupposes a unifying relationship of reciprocal knowledge, which works to bridge *spatial* distance. Transmission, on the other hand, is a media function through *time*. This time-axis orientation of transmission enables a number of unusual media capabilities. For example, cryptographic technologies divide and control for time, so that time can be manipulated. For instance, messages can be encrypted so that only *future* cryptanalysts can read the message. Or consider the "proof of work" feature of the cryptocurrency Bitcoin, which uses the statistical regularity but computational difficulty of finding a hash collision to precisely set a mining "difficulty" level, which appears random, since there is no tractable way to determine when a solution (hash collision) will be found, but ultimately, at the level of the Bitcoin network, the outcome is predictable. The transmission process of encryption excels at time-axis manipulation.

---

[12] See chapter eight for a discussion of transmission, chapter nine for a discussion of the role of cryptanalysis, and chapter ten for a discussion of the Other in ciphertext.
[13] Krämer, *Medium, Messenger, Transmission*, 19.
[14] Ibid., 22.
[15] Enns, "Introduction: The Media Philosophy of Sybille Krämer," 14; Kittler, *Gramophone, Film, Typewriter*, xxxix.

Consider, moreover, how the notational epoch used plaintext technologies for memory. Memory is a form of transmission across time. Therefore, encryption devices are mnemonic because they send messages into the future (to be decrypted later) and reach into the "deep time" of past media. There are many unsolved coded messages which offer poignant examples of the "deep time" of media. The most florid and famous of which is the Voynich manuscript, still unsolved after hundreds of years of sustained human attention. Many other, more banal examples exist too, such as the routine diplomatic correspondences of literate cultures, or, as is commonplace today, encrypted data stores too mundane to bother storing for posterity, much less being worthy of cryptanalytical attention (one can only imagine how much encrypted data the NSA has stored for future intelligence gathering).[16]

Transmission also requires a material conversion. There can be no "transmission of movement, in the mechanical sense," Debray writes, "without machine parts that produce it."[17] This movement might occur with the energized silicon of a transistor, the turn of an encrypting rotor, or the movement of a pencil across paper—each with their own process of material conversion necessary to perform the transmission function. Material conversion is also associated with communication media, necessary for spanning real distance, as well as for use with mnemonic technologies. These mnemonic technologies were invented, according to Debray, to transmit meanings, that is, a process of transmitting "culture." We transmit culture so that the "things we live, believe, and think do not perish with *us* (as opposed to [perishing with] *me*)."[18] According to Debray, this implies that there are, strictly speaking, no "transmission" machines but only tele-transmission machines working across time.[19] Thus, we might consider, to encrypt a message is to transmit culture to the future.

7.2 Perception and encryption

It took a "discovery and decryption," according to Zielinski, to confirm Empedocles' theory of media.[20] In 1997, two papyrologists unearthed a forgotten papyrus fragment and discovered, after much analysis and reconstruction, that it belonged to a longer text of Empedocles. What the decryption revealed was

[16] For the concept of the deep time of media, see Zielinski, *Deep Time of the Media*.
[17] Debray, *Transmitting Culture*, 7.
[18] Ibid., 3.
[19] Ibid., 5.
[20] Zielinski, *Deep Time of the Media*, 39.

Empedocles' account of his theory of perception, a synecdoche for his absent theory of media. According to the Empedoclian fragments, a fine skin or film covers all matter, which contains invisible pores that constantly emit effluences in all directions. When an effluence of the right size meets a compatible pore in another material, sense perception occurs (this process extends beyond human sense perception to include plants and animals, and possibly all matter).[21] However, Empedocles does not believe that any intervening material medium is necessary—it is as if the object touches the sense organ "directly" through the effluences. In fact, there is, we might conclude, no media in Empedocles' media theory.

Democritus built on Empedocles' media theory of pores, introducing two important refinements: a void, and a material "between." For Democritus, all matter is made of imperceptible atoms that exist within a void (the void is necessary so that the atoms can move about). As these atoms move through the air, from an object to a sense organ, they are compressed to take on various constellations, images, or "idols" (*eidola*).[22] When the resulting image contained within the compressed air makes contact with the appropriate sense organ, perception of that object occurs. Democritus thus introduced the concept of media in his theory of perception, but because the object and subject are separated in space and only joined by imagistic idols, false images become a necessary danger. Diogenes Laertius opinion of Democritus' theory, was that "we know nothing [of the world], for the truth lies in the abyss."[23] Democritus' view is in this way much like McLuhan's famous dictum that "the medium is the message," whereas Empedocles offered a way of understanding how a "between" can function without distortion, ideology (i.e., *eidola*), or falsehood.

But such a media theory seems impossible. We know that media require a material substratum. In fact, in chapter five I discussed how the ideality of notation requires marks and inscriptions. Empedocles' theory, however, offers us an opportunity to recognize how theory sets both the upper limit and ultimate goal for the medium of encryption. In a perfect and ideal world, encryption would be a relatively simple combinatory problem: a "set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms)," as Shannon remarked.[24] Such a world will never exist, but it was often dreamed.

---

[21] Ibid., 46.
[22] Ibid., 51.
[23] Ibid., 52.
[24] Shannon's genius, however, was to recognize that while mathematics might effectively model encryption it was at the end of the day an engineering challenge. Shannon's recognition of the

7.2.1 The medial limits of encryption

The dream of perfect media (media without media) made possible by encryption has probably existed since antiquity. In part one I described the effects of many scientists and scholars who turned to cryptography and cryptographic apparatuses in an attempt to develop commodious forms of writing. For instance, Gaspar Schott's description of cryptographic writing in *Schola steganographica* (1606) was exemplary in this regard. In this work he imagines that air can act like a mirror by receiving and retaining impressions of objects (and even speech). Much like Empedocles' pore theory of perception, Schott thought that the mimetic transference (the specular impressions) could occur at any distance and would work relatively quickly—within a day the recipient's mind would be informed, whether the recipient was awake or asleep. Unlike some of the other proposals of the time, such as Wilkins', Schott did not require the interventions of a messenger or even a medium; his communication scheme worked "without the mediation of any spirit."[25] Similarly, Trithemius' student and fellow occultist, Agrippa, also described a "metaphysical telepathy with the aid of celestial impressions" in his *Occulta philosophia* (1533).[26]

The belief in perception free from mediating materials did not end with the supposed rise of scientific thinking after the Enlightenment. In the nineteenth century, Edgar Allan Poe was so fascinated by cryptography and emerging communications technologies that these technologies became central figures in his poetry and prose. Poe's interest was unusual among literary figures because, while he failed to carefully demarcate between a loose, lyrical sense of "crypt" as a kind of mysterious stuff and more specialized cryptography, he did actually *use* "proper" cryptography in some of his writing.[27]

---

role of physical entropy was as practical to his information theory as it was his theory of cryptography. See Shannon, "A Mathematical Theory of Cryptography."

[25] The claim to have developed a commodious communication scheme without the use of an intervening spirit was in part a conceptual requirement, but also a political dodge to avoid (all too common) accusations of demonology.

[26] Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia."

[27] My intention is not to draw too fine of a line between the metaphoric use of "crypt" for literature and "cryptography" for the serious stuff that military and high-technology pursues. Rather, my point is that a distinction *can* be maintained. The distinction I want to maintain is between notational forms of plaintext that extend into encryption, and other linguistic forms of "cryptic" writing that work on the level of metaphor. (Derrida's foreword to Abraham and Torok's psychoanalytic work is a fine example of the multivocality of "crypt," "cryptic," and "encrypt"; see Derrida, "FORS.") For instance, this distinction extends to research on hieroglyphic writing. Hieroglyphic writing fascinated early cryptographers, who believed it was encrypted, until the discovery of the Rosetta stone proved that is was a natural language.

Poe's theory of cryptography relies on the baroque nature of human cryptanalysis and its mimetic representational structure. In "The Gold Bug," the main character Legrand solves the complex perambulations of a monoalphabetic cipher and multiple layers of representational interpretation by arranging the forces of mental intuition and material circumstances. The cipher is "super-encoded" on account of being rough and rude, and in a faint red tint. The resulting riddle only solved by interpreting multiple puns and metaphors, and ultimately, by getting the slave Jupiter to climb a tree and thread a gold scarabaeus through the left eye of a skull fastened in the tree.[28] Similarly, in "The Purloined Letter" the character Dupin recalls the process told to him by a child who was able to consistently make correct guesses at the game of odds and evens:

> *When I wish to find out how wise, or how stupid, or how good, or how wicked is any one, or what are his thoughts at the moment, I fashion the expression of my face, as accurately as possible, in accordance with the expression of his, and then wait to see what thoughts or sentiments arise in my mind or heart, as if to match or correspond with the expression.*[29]

Like Schott's specular theory of cryptography and Empedocles' theory of perception, these processes of cryptanalysis work by impossible transference of mental states—an interpretive, mimetic representation without media. The face card offers a solution to the problem of the relation between mind and body, and the problem of other minds, by becoming a literal *face* card.[30]

Poe believed that encryption was both transmission and communication. In correspondence with Poe, one reader suggested that cryptography was useful to "secure… the conviction that the magic scroll has a tale for my eyes alone. Who has not longed for such a confidante?"[31] This telling description posits a utility to encryption that does not require communication across distance, but rather, encryption being used to transmit to a future self. In this case, encryption is purely temporal. But Poe was also deeply interested in the invention of the

---

Discovering that hieroglyphs were a natural, written language (partially alphabetic, no less), did not stop commentators from suggesting that, while they may not have been "encrypted" as sometimes imagined, its discovery was a process of cryptanalysis. For example, Abraham Sinkov's *Elementary Cryptanalysis: A Mathematical Approach* suggests that cryptanalysis was essential to the reconstruction of lost languages—languages so lost that they were in effect "secret languages" (i.e., encrypted); see Rosenheim, *The Cryptographic Imagination*, 54.

[28] Poe, *The Gold Bug*, 49.

[29] Poe, "The Purloined Letter" quoted in Rosenheim, *The Cryptographic Imagination*, 26.

[30] Ibid., 29.

[31] W.B. Tyler quoted in Ibid., 34.

telegraph, a communications technology invented and popularized in his lifetime. The telegraph introduced a communications medium for cryptography, which tied encryption and communication very closely together. More than even before, the telegraph was, in a single strike of the Morse key, both an encryption and a medium, that is, a prosthetic extension across space and time.

The ultimate goal of telegraphy, which lived on in the popular imagination of the technology, was the annihilation of distance and instant communication. Poe's fascination with the technology led to his support for its development, and his belief that Morse code was a metaphor for good writing.[32] In fact, in an effort to realize the ultimate goals of this mysterious technology, an 1842 bill appropriating thirty thousand dollars for the construction of a telegraph line from Baltimore to Washington would prove politically divisive because the politicians who backed the construction saw great promise in the telegraph technology but, hedging their bets on the unproven technology, they also thought it prudent to allocate half of the appropriated funds on the "scientific analysis" of the "magnetism of mesmerism."[33] In the politicians' and public's minds, the telegraph was not really a material media technology, but more alike to the technology of mesmerism, as an extension of sense perception and communication without media.

This cryptographic theory of perception, working without media, was no more clear than in the works of spiritualist Lizzie Doten, who in 1862 published a collection of works "dictated" from transmissions of Poe from beyond the grave. Doten's transmissions cannot be said to be "properly" cryptographic, instead they are "secret" codes, but they do reflect the cozy associations between telecommunications technologies and perceptual models of media. Or, consider how famous "mediums" like the Fox sisters relied on a "spiritual telegraph."[34] These spiritual telegraphs used a code language similar to Morse code (often comprised of discrete knocks), which not only spanned distant lands at a rapid pace (like the material telegraph), but also connected to past times and ethereal realms. In this way, the "medium" was no medium at all, but rather the sense organ appropriately configured to receive cryptic messages.

❦

The encryption process is perhaps the most distinctive part of cryptography. Indeed, the various encryption algorithms are used to demarcate and distinguish between one kind of cryptography and another, and research and development

[32] Ibid., 92.
[33] This was, perhaps, intended as a joke. Ibid.
[34] Ibid., 119.

in cryptography focuses almost entirely on this important aspect. Beyond instrumentalist notions of algorithmic diversity, the curiously distinctive feature of encryption is its ability to function as a medium. This chapter introduced the idea that encryption is the "primal scene" of cryptography because it sits between source and destination, or object and subject, just like media. As either communication (over distance) or transmission (over time), encryption has an important mediatic role to play. Due to the seeming sensitivity and yet raw power of cryptography, the limits of media were sometimes explored by using encryption processes, with authors envisioning novel ways of augmenting perception to become more subtle and finely tuned. Like the telegraph and other communication devices, encryption was a prosthetic technological medium that enlarged the human limits of perception.

Such media effects oftentimes required some other co-determinate technology, such as the telegraph, to aid in the process. When coordinated with another technology, encryption increases the media capabilities of the underlying technology. In fact, a case can be made for the conclusion that, without encryption, many of these communication technologies would have been practically deficient and would not have been further pursued. With no codes to transform natural language into compact, commodious forms of writing, the benefit of many technologies would have been vastly diminished.

These media effects, however, did not just enable encryption to reach out into the world and communicate across time and space. Media effects are, in fact, essential to the very functioning of encryption itself. Cryptography encompasses two vastly different worlds: due to its notational properties, plaintext is an exceedingly constrained form of writing, while ciphertext has the appearance of pure chaos. The gulf between the two is so enormous that processes of encryption must—necessarily—transcribe movement *between* the two worlds.

8
Communication and Transmission

> *Each angel is a bearer of one or more relationships; today they exist in myriad forms, and every day we invent billions of new ones. However we lack a philosophy of such relationships.*[1]

Capurro, Debray, Serres, and Krämer, and more recently Galloway, Thacker, and Wark, each in their own way, have made messenger angels central figures of their media theory.[2] In doing so, these writers have worked to move beyond the narrow conceptual limits of media set by Shannon's instrumentalist conception of information, instead, they explore literary, cultural, economic, and power relations within a message or messenger theory of media. Even if today such ethereal ontologies have been replaced with scientism, and are now deeply proscribed, this metaphor still has a long and vibrant past in cryptography. The metaphor, and myths, of angels was often used to understand how encryption functions as a medium between plaintext and ciphertext. This chapter provokes existing conceptualizations of encryption by exploring a conceit: that the mythic existence and functioning of messenger angels can explain how the process of encryption works. The result of this chapter is a reassessment of conventional descriptions of encryption, made possible by a typology of encryption that works though messenger angels.

Johannes Trithemius (1462-1516) was probably the first author to use an angelic metaphor to describe cryptography, and due to his vast influence, the angelic messenger quickly became a common theme for cryptographers looking to understand how encryption can transport messages rapidly, across great distances, in secret, and with efficient or commodious means of writing.[3] John

---

[1] Serres, *Angels, a Modern Myth*, 293.

[2] Capurro, "Angeletics: A Message Theory"; Capurro and Holgate, *Messages and Messengers - Von Boten und Botschaften*; Debray, *Transmitting Culture*; Serres, *Angels, a Modern Myth*; Krämer, "Messenger Angels: Can Angels Embody a Theory of the Media Avant La Lettre?"; Krämer, *Medium, Messenger, Transmission*; Galloway, Thacker, and Wark, *Excommunication*.

[3] Gaspar Schott (1608-1666) rebuffed the occultists who looked to Trithemius' work, warning that only simple-minded people would believe that Trithemius and his followers were speaking about "real spirits and teach that real conjurations are to be offered and that the summoned spirits actually respond." Schott might have discounted the existence of real spirits, but he certainly believed that encryption was a powerful technology. See Shumaker, *Renaissance Curiosa*, 107.

Wilkins (1614-1672) later titled his cryptography manual *Mercury: or, The secret and swift messenger,* a reference to the Roman name for the Greek messenger angel Hermes. Wilkins' work was deeply indebted to Trithemius and his angelic metaphors. As accusations of demonic magic became increasingly dangerous, Athanasius Kircher (1602-1680) responded by producing a description of encryption media that was nonetheless a safe distillation of Trithemius' work. Despite having no references to angels or spirits, Kircher's distillation, never ruled out the possibility of transmission media that worked by the invisible forces of magnetism or other occult, but not necessarily demonological, properties.

Although serious scientific investigation of encryption no longer needs the explanatory power of angelic messengers, this does not mean the myths of angels are not worth studying. Contemporary media theories that interrogate the myths of angels do so with the conceit that myths can, and should, be taken very seriously. The mythic is still very alive in contemporary discussions of technology. Mosco has identified this impulse with the "technological sublime."[4] Moreover, with so much contemporary attention being paid to angels in media theory (half a dozen leading theorists attend to the subject), there is a strong signal suggesting the possibility that angels may offer conceptual inroads to the study of encryption. Critically, the functional myths of angels provide rich descriptions of the ways that the vast gulf between plaintext and ciphertext can be bridged. Contemporary myths of technology rarely supersede their past.

Alternatively, we could rekindle an idea popularized during the Renaissance and early Modernity—recognizing that angels were not supernatural beings, but rather merely created beings that are rare, and thus special.[5] The difference between the Renaissance and today, however, is that encryption—and the "angels" necessary for its functioning—are no longer rare. The reason, we might concede, is that we no longer live in rare times—angels are everywhere and ubiquitous, as found in high technology.

8.1 THE ANGEL IN THE MIDDLE

To understand media as a middle, third, or "between" function,[6] a natural connection with angels and media theory emerges, which has recently been explored by prominent media scholars. To various degrees, these scholars align

[4] Mosco, *The Digital Sublime*.
[5] Daston, "Preternatural Philosophy."
[6] See chapter seven for a discussion of the roots of, and need for, understanding media as a middle function.

the myths of angels with media technologies, and explore the functions, capacities, and processes of media through these references.

Capurro uses the term "angeletics" to describe his media theory, preferring this neologism to the more conventional "angelology." Angeletics, according to Capurro, is a specific restriction of topic and method of study. The approach investigates only human messages and human messengers.[7] Serres, on the other hand, takes a more speculative approach, extending his analysis beyond human hermeneutics—seeing angels all around, in the networks of global transportation and media technologies.[8] Serres' characterization is, therefore, mythical yet embodied in starkly concrete things and places. Similarly, Debray invokes Victorian media technologies in his study of angels, calling them "the little telegraphists of the Almighty."[9] For Debray, angels occupy a third position, as a medium between the sender and the recipient of a message. Krämer's approach, different still, focuses on the etymological connections between angels and message technologies, noting that the Greek word *"angeloi"* is derived from the name of the Persian postal service; and in Greek, Hebrew, Arabic, and Persian, "angel" is the term for the function or activity of a messenger[10] (or ambassador).[11] Krämer argues that angels can provide a model for the "technical-informative exchange" of routes and messages, which avoids the typical binary of media studies—between living, communicating beings and the machinations of high technology.[12] Most recently, Galloway has focused on the effects of angels in the middle of mediatic relationships, with each middle having its own angelic avatar and corresponding characteristics.[13]

In this chapter, starting with Capurro, I will describe each of these myths of contemporary media theory as it relates to the processes of encryption. In doing so, I will draw out the ways that angels offer a model for understanding the complexities of encryption, and a site of theoretical investigation.

For Capurro, the angelic avatar is Hermes. Capurro explores Hermes' myth to develop a "second order hermeneutics,"[14] which is about messages in a postal

---

[7] Capurro, "Angeletics: A Message Theory."
[8] Serres, *Angels, a Modern Myth*.
[9] Debray, *Transmitting Culture*, 32.
[10] Krämer, "Messenger Angels: Can Angels Embody a Theory of the Media Avant La Lettre?," 221.
[11] Krämer, *Medium, Messenger, Transmission*, 87.
[12] Krämer, "Messenger Angels: Can Angels Embody a Theory of the Media Avant La Lettre?," 222.
[13] Galloway, Thacker, and Wark, *Excommunication*, 29.
[14] Capurro, "Angeletics: A Message Theory." The word "hermeneutics" is derived from the same root that gives Hermes his name.

model,[15] and (only in a secondary sense), "an interpreter and translator."[16] Capurro's approach makes a lot of sense when considering the media of encryption. First, as I explore in chapter nine, interpretation and translation are transformations that are ontologically and methodologically distinct from encryption and decryption. Second, as an angelic model for encryption, the characteristics of a postal model are essential to how encryption can perform transformations without semantic alteration. That is, if any interpretation or translation were to occur, the message would be altered, and would therefore destroy constitutive notational identities—resulting in destruction, not encryption.

Hermes can post messages without interpretation or translation because unlike other reciprocal media functions (dialogue and information), on the postal model, messages are "sender-dependent" and asymmetrical.[17] Unlike theories of information, which presuppose that information is requested, the postal model recognizes that messages are simply received. To explain how messages can be received, Capurro invokes Luhmann's communication theory, which distinguishes between messages (the act of offering something), information (the process of selecting from a range of possibilities), and understanding (the integration of meaning into the system). For dialogue in a natural language (i.e., not encryption), the selection from a range of possibilities involved in the transmission of information requires a common understanding (both parties must speak the same language). Such a common understanding is impossible for encryption, of course, because plaintext and ciphertext are unlike each other in important ways (plaintext and ciphertext are not in the same "language"). Messages, on the postal model, must follow a "principle of respect," a "principle of faithfulness," and a "principle of reservation."[18] That is, messages must be "new" (in the Luhmann/Shannon sense of information as unexpected and relevant), *undistorted*, and passed without interpretation. These requirements of respect, faithfulness, and reservation dramatically change the relationship between sender and receiver.

If we translate Capurro's hermeneutical analysis into the language of a technical media theory, we can see how these three principles may exist in technical protocols and interfaces.[19] Respect, faithfulness, and reservation become the practical requirements for message transmission—dictating how,

[15] Ibid. Krämer seems to have developed her postal principle from Capurro's writing.
[16] Capurro, "What Is Angeletics?"
[17] Capurro, "Angeletics: A Message Theory."
[18] Ibid.
[19] Cf. Galloway, *The Interface Effect*.

when, and if transmission occurs. Consider, for example, how Internet transmission protocols re-encode "best effort" norms, or how analog to digital conversion algorithms create the illusion of faithfulness to the original. Encryption protocols, however, work to remove any common ground between plaintext and ciphertext, *reconfiguring* the message itself. Therefore, on this model, we can recognize how the process of encryption is a really a radical transformation without a common understanding.

But why is the transformation *radical*, at the exclusion of dialogue, or the communication of information, which both require a common understanding? How does the radical transformation reconfigure the protocological message passing function, changing the principles of respect, faithfulness, and reservation into shadowy, veiled operations? As a mediatic middle, encryption transformations are radical because human phenomenology is incapable of bridging the gap between the natural expressiveness and interpretability of plaintext and the perplexing, technically-mediated nature of ciphertext.[20] While there is no necessary guarantee that plaintext makes sense to all people (for example, to the illiterate), it does *permit* itself to be made sensible. Ciphertext, on the other hand, is precisely the opposite. Ciphertext actively resists being comprehensible. The point of encryption is to eliminate any phenomenological routes (no common understanding) to move from plaintext to ciphertext, without the appropriate kind of technical mediation.

The message-passing function of Hermes is critical to the postal model of encryption because his myths reimagine traditional message transmission processes. In fact, Hermes acts as the protocological method of information channel transmission, crossing the radical gap between plaintext and ciphertext because he (asymmetrically) *sends* messages from plaintext to ciphertext, and (asymmetrically) back again from ciphertext to plaintext.[21] Hermes' function is not that of a stable "common understanding," but rather, as an active, hybrid, and independent figure of transmission. Encryption is a reconfiguration of message transmission, but significantly, not a process of dialogue or information communication.

[20] The totality of ciphertext includes, in a subaltern way, the decrypting algorithm, physical materials and marks, mathematics, and other such parts that enable the transposition and substitution of notation. See part three for a full discussion of ciphertext.

[21] In this regard cryptanalysis—code breaking—short-circuits Hermes' transmissions, and is an extension of linguistic decoding, as described in chapter nine.

Since encryption is fundamentally a technical process, it makes sense that Serres considers Hermes a precursor to information theory.[22] For Serres, angels are a metaphor for technological networks, flight paths, telecommunications, logistics, and many other transmission technologies. These angels occur everywhere messages transmit—that is, today, everywhere.[23] Although Hermes is usually depicted in human form, with his cloak, round hat, and winged staff, Serres notes, "in the oldest traditions, angels do not necessarily take on human appearance; they may also inhabit the universe of things, whether natural or artificial." Critically, angels embody and "make possible our message-bearing systems."[24] Serres believes we are heading towards a "new [mediated] universe," on the "wings of angels, who are its workers."[25]

8.2 ENCRYPTED TRANSMISSIONS

Despite the promise of telecommunications technologies, the "new universe" Serres identifies did not necessarily result in the death or even compression of distance. More than ever, it seems, geography matters. For high technology industries, highly skilled workers move in droves to technopoles. Workers move to technopoles *despite* the capabilities of telecommunications technologies and access to telework, *not because of* concentrations of these technologies. As a global medium, the infrastructural expansion of cryptography is parasitic on the expansion of telecommunications, and the effects of communication at a distance. Therefore, encryption is vital for widespread, secure communication. However, in terms of media theory, encryption is fundamentally a process of *temporal* transmission.

The distinction between telecommunications technology, with it spatial model, and encryption, with its temporal model, is often ambiguous and co-determined. Indeed, telecommunications and encryption work together and yet to different ends.[26] Ernst offers a media-archeological parallel to the co-

[22] In discussing Serres' vision of angels as precursors to information theory, Krämer describes a resemblance between Serres and Helmut Wilke, who believes that angelic transmission has been replaced by "megamachines of information processing." See Krämer, *Medium, Messenger, Transmission*, 88.
[23] Serres, *Angels, a Modern Myth*, 8, 52.
[24] Ibid., 166.
[25] Ibid., 297.
[26] The existence of cryptography and its ability to transmit into the future complicates Innis' classic distinction between heavy and durable communications technologies (such as architecture and stone engraving), and ephemeral and light communications technologies (paper and telecommunications technologies). According to Innis, the heavy technologies transmit into the future, whereas the light ones transmit across space. Cryptography is precisely

determination of mediatic encryption and telecommunication: "transfer and storage are two sides of the same coin: storage is a transfer across a temporal distance."[27] The ambiguity of storage and transmission across time is also fundamental to cryptography; cryptography *can* be connected to communication devices, but is essentially the duality of storage/transmission. Consider how this feature of cryptography reveals itself: when engineers speak of the "strength" of an encryption algorithm they often measure it in key bit-length and the amount of time current computing resources would take to crack it. Therefore, encryption provides ciphertext, which transmits a message into a future world, where it can be either decrypted or cryptanalysed. This time criticality is essential to understanding the media effects of encryption, as well as for determining engineering outcomes.

A reimagination of the postal model—sending across time rather than space—also recommended by Boyne, which offers a fitting description of the activity of encryption. Boyne argues that the present is an infinite series of possibilities constantly sending messages to the future.[28] With Boyne's model of time, as part of the postal model identified by Capurro, protocol and exclusion turn out to be necessary features of transmission. Moreover, Boyne reads the concept of an archive as an archive of the future—the route of angelic transmission.[29] By constantly sending messages to the future, the metaphor of the angel permits multitudinous and temporal possibility. But, Boyne remarks, the archive is oriented towards access or exclusion, just like encrypted messages. "Certain memories," Boyne writes, are ruled "out of play," as the archive must make selections from the infinitude of reality.[30] Therefore, in terms of media transmission to a future, encryption is the process of exclusionary transmission into an archive.

Through encryption, we cannot understand the exclusion of the future world, so angels are also needed as "bringers of the Word… until it arrived, in the flesh."[31] The angels that transmit the Word to "the flesh" invert the exclusions, and therefore decrypt messages. As ciphertext is decrypted into plaintext, the message again becomes phenomenologically accessible, and potentially meaningful. In this middle, mediatic space, moving from plaintext to

---

the inverse: as light as any communication technology, and yet transmits essentially into the future. See Innis, *Empire & Communications*, 7.

[27] Ernst, *Digital Memory and the Archive*, 100.

[28] Boyne, "Angels in the Archive," 211.

[29] Ibid., 216.

[30] Ibid., 215.

[31] Serres, *Angels, a Modern Myth*, 9.

ciphertext, and back, angels enable humans to see "the differences between worlds,"[32] but without collapsing the "networks" of possibilities, connections, and strategic alliances.[33] This act of angelic "conversion," which requires "amphibious keys" or an "interchanger," might be telecommunication equipment or encryption and decryption routines.

Another mythic characteristic of angelic transmission is the act of disappearance. Serres tells a story of "Gabriel," an (angelic) old homeless man who lives in the airport. According to Serres' parable, in his dying moments, Gabriel offers a message of peace, then expires.[34] This theme of transmission-then-dying is central to messengers. Krämer also recalls the runner from Marathon, who delivers the message of Athenian victory and then immediately drops dead.[35]

This act of disappearance is a special function of the transmission of messages. In typical (communication) media circuits, the medium is always at risk of overwhelming the message. But in message *transmission*, the medium must show restraint, delivering the message without interpretation or censure. For the transmission process involved in encryption and decryption, a balance between restraint and transformation is needed. There is no message transmission without some transformation of voice or flesh: "it is necessary for… [the messenger] to appear and speak, in order to deliver the message!"[36] Not speaking—the silence of ciphertext—is no transmission at all. But media that dazzles risks interfering with the encryption and decryption functions. "This is," Serres argues, "the question of the intermediary: if he is too magnificent, he may intercept the message; if he is too discreet, he won't make it heard."[37]

In recent years (it has not always been the case),[38] encryption and decryption have become homogenous processes, as the needs for reusable cryptography have increased. The demands for "industrial" applications of cryptography has led to the development of reusable encryption algorithms that differ only with respect to their keying material and (sometimes) the source of (pseudo-)random information. This multiple, reusable mediation is also a function of the angelic

[32] Ibid., 166.
[33] Ibid., 170.
[34] Ibid., 20.
[35] Krämer, *Medium, Messenger, Transmission*, 37.
[36] Serres, *Angels, a Modern Myth*, 104.
[37] Ibid., 101.
[38] The cryptographic "key" that we are familiar with today was probably invented by Bellaso in 1533; see Buonafalce, "Bellaso's Reciprocal Ciphers."

messenger: "since an angel is himself a skeleton key, he offers something even better: a whole bunch of keys!"[39] And this is precisely how modern encryption works: one skeleton key in the form of the encryption algorithm, which locks and unlocks as many plaintexts and ciphertexts as there are individual keys.

The distinction between encryption/decryption and cryptanalysis,[40] which I discuss in chapter nine, can also be found in the angelic metaphor. Messenger angels are necessary to "announce" or send God's Word to all beings, just as messengers announce or cryptanalyse from unbounded ciphertext to a singular, specific plaintext. Similarly, consider the parallels with encryption. According to the myths, Hermes is a lying, cunning figure who knows how to hide and is therefore able to disguise code.[41] As the god of orators and also the god of thieves, Hermes knows how to manipulate (to *encrypt?*) natural language. Hermes is even more powerful than Calypso, "the one who hides," which suggests a primacy of mediatic encryption over the powers of obfuscation.

In sum, the role of messenger angels for encryption is fourfold: First, encryption is always derivative, in the sense that it disappears in transmission. Second, the encryption process is invisible and hybrid because its production and transmission occur at one and the same time. Third, encryption is a necessary "exchanger" between the worlds of plaintext and ciphertext, because these worlds are too radically apart to permit any semiotic connections. Fourth, the encryption process is multiple and homogenous.

Krämer focuses on several aspects of angelic transmission not yet discussed. I have reduced her more extensive list to the three most relevant: 1) embodiment, 2) hybridization, 3) and demonic inversion.[42] So, how does encryption factor into these aspects of the transmission event?

The embodiment of angels is paradoxical, for their *conditio sine qua non* is their materiality, but they also "embody" incorporeality. Without bodies they "would not be angels at all, but rather like God himself."[43] Yet angels dissolve into light or air, as a "spiritual physicality."[44] Angels use their paradoxical embodiment to mediate between humankind and God. "Is there anything more

[39] Serres, *Angels, a Modern Myth*, 293. Serres appears to misinterpret skeleton keys, which are single keys capable of opening many locks. The angelic messenger is really a "whole bunch of keys," as Serres also describes.
[40] See chapter nine for a discussion of why encryption/decryption and cryptanalysis are formally, functionally, and analytically distinct.
[41] Serres, *Hermes: Literature, Science, Philosophy*, xxxiv.
[42] Krämer, *Medium, Messenger, Transmission*, 90–93.
[43] Ibid., 90.
[44] Ibid.

distant and different from one another," Krämer asks, "than God and man?"[45] The *confusio* that God cast upon humankind for constructing the tower at Babel was possibly punishment for the hubris of attempting to close this gap. As with all technologies, encryption speaks on behalf of others—angels do not act on their own impulses[46]—they are simultaneously empty yet "bearing witness." Encryption thus offers a kind of absolution, speaking on behalf of the author but "plausibly deniable," as cryptography products such as TrueCrypt demonstrate.[47]

In order to take part in both worlds—divine and corporeal—angels must be hybrid creatures with properties from both worlds. Angel hybridity comes in the form of weightlessness, yet wingedness; comprehension of the infinity of God, yet the ability to "speak" in human terms. This hybridity could be accomplished through the dialectical synthesis of the two worlds, giving rise to a "higher" one. But, according to Krämer, this is not how angelic hybridity works. Rather, angels "unite on the same plane."[48] For encryption, the hybridity and unification is its relationship to noise. When encrypted, a message approximates noise, and in some cases, may even be formally indistinguishable. Thus, for encryption, weightlessness/wingedness and speech/infinity hybridity comes together on the plane of noise.

But, as we know, the angel that desires to be too close to God is hurled to Earth. This demonic inversion is a "suspension of the mediator's position."[49] Lucifer's fall bears witness to his forsaking and is a rejection of the hybrid world of mediators. What Lucifer is left with, Krämer notes, is not the transmission of messages but "the purchasing of souls through the exchange of services in a demonic pact."[50] For encryption, the suspension of its mediation function results in the activities we call cryptanalysis. In a "normal" operating environment, the mediation provided by message transmission—encryption—speaks and produces itself in one breath, an implicit guarantee that the message is honest. By suspending mediation, the hubris of hermeneutics identified previously by Nietzsche is introduced and makes guesses about the true meaning of messages. Falsehood, and the possibilities of illusion through

[45] Ibid., 89.
[46] Ibid.
[47] TrueCrypt was an important open-source cryptography product from 2004 until 2014. It offered its users the ability to create a hidden—and further encrypted—partition within an encrypted volume, so that if required to turn over the cryptographic keys the user could comply, but plausibly deny that a further (undetectable) partition existed.
[48] Krämer, *Medium, Messenger, Transmission*, 91.
[49] Ibid., 92.
[50] Ibid.

mimetic realism, become genuine concerns. Cryptanalysis, therefore, is a technological version of demonic inversion, commonly realized in the glory of hackers, crackers, and "black hat" engineers.

8.3 From Hermes to Iris

Hermes is the avatar for hermeneutics, but as we saw in chapter five, in the discourse network 2000, hermeneutics is in crisis. Hermeneutics is in crisis, according to Galloway, because there are now many strategies and technologies that side-step the interpretive impulse. "Why try to interpret a painting," Galloway asks, "when what really matters are the kinds of pre-interpretive affective responses it elicits—or, to be more crass, the price it demands at auction?"[51]

Galloway provides a diagrammatic explanation of mediation focusing on three processes: exegesis, hermeneutics, and symptomatics.[52] With exegesis, interpretation typically runs "with the grain" and is usually broadly sympathetic to the author's intention. This is *logos* in its workaday sense, associated with dialogue and mutual grounding. Dialogue is a characteristic form of exegesis, but in order to maintain communication, the participants must share linguistic, social, and psychological characteristics, and be broadly charitable to the other's position. Combative or interrogative dialogue is only possible and productive in certain constrained circumstances. Dialogue with an interlocutor who consistently misinterprets your meaning, either through malice or error, inevitably results in an almost complete breakdown of communication. Hermeneutics, on the other hand, runs "against the grain" of literal truth, and tries to "unmask" inner realities. The myths of Hermes as a merchant and messenger is poignant here, since "hermeneutics assumes that the work itself is a foreign land that must be visited."[53] Hermeneutics challenges the assumption that the truth revealed by exegesis is plain and true, and not somehow false or obfuscatory. Hermeneutics is associated with cryptanalysis, focusing on linguistic interpretation and subtle clues. Symptomatics, on the other hand, rejects exegesis and hermeneutics completely, and instead reads the surface facts as clues to absences, contradictions, and misunderstandings.[54] Symptomatics are

[51] Galloway, Thacker, and Wark, *Excommunication*, 29.
[52] Galloway, "Love in the Middle," 37.
[53] Ibid.
[54] Ibid., 39.

orthogonal to the encryption/decryption dialectic, and instead insinuate "the whole framework of knowledge" as something "obsolete."[55]

If Hermes is the angelic avatar for cryptanalysis because of his cunning, concealing, and interpretive ways, who is the avatar for encryption and decryption? A second mode of mediation, one exemplified by Iris, is a good candidate. Iris is the goddess of the rainbow, and along with Hermes one of the two messengers to the gods. Whereas Hermes is full of complexity and is the subject of multiple myths giving him many characteristics (god of animal husbandry, roads, travel, hospitality, heralds, diplomacy, trade, thievery, language, writing, persuasion, cunning wiles, athletic contests, gymnasiums, astronomy, and astrology), Iris has no mythology of her own.[56]

Iris is a swift messenger, the handmaiden and personal messenger to Hera, queen of gods. Her name comes from the common roots of "speaker" and "messenger," but her name might also be related to *eirô*, "I join," which also works as a functional description of her mediatic role between two distant worlds. Iris is "pure relay, carrying and repeating messages," but her retelling is often different from the original.[57] She doubles the message, not unlike Dupin in Poe's "The Purloined Letter," who doubles the face card with his face to decipher the other's poker hand (see chapter seven). With Iris, however, sometimes the doubled message is different from the original. This is not due to interpretation (Iris does not interpret messages). Rather, Iris writes messages down—she *remembers* them—and is selective about which messages are relayed, and how (this is the protocological, exclusive function of encryption). That the doubled message is sometimes different from the original is due to Iris' mnemotechnical nature, choosing to remember her messages—to become a literal medium—rather than write them down.

Galloway calls Iris' mediation "iridescent," a unidirectional sending of "absolute *certainty*."[58] Galloway speaks of the future of Iris in prescient terms, as her myth relates to the future of cryptography: "Iris *can and will be mathematized*."[59] Indeed, the mathematical properties of Iris are increasingly subsuming the mythic powers of Prometheus, the inventor of fire and a symbol of technicity. Increasingly, the myth of Prometheus is being replaced with Iris'

[55] Ibid.
[56] "Theoi Greek Mythology."
[57] Galloway, "Love in the Middle," 42.
[58] Ibid., 41.
[59] Ibid., 45.

mathematized message transmission—"we are employed principally in transmitting messages," now encrypted.[60]

❦

The parallels between encryption and angels are numerous: Angels transmit messages without interpretation, while excluding outsiders. Encryption is the same, ignoring meaning so as to reorder the message, that only intended recipients can read. The angel must ensure that it passes the message and dies, so as to not dazzle the recipient. Encryption is a medium that is silent and nearly invisible. Angels remember messages to bring them across time—to the future or leave them in the past. Encryption safeguards data for posterity, or ensures that only future people's will be able to read the message when sufficiently advanced cryptanalytic technologies are developed (Only when paired with communication devices can encrypted messages be passed across space). In order to perform these functions, angels must be hybrid. Encryption approximates noise, allowing it to produce more (apparent) noise. Angels are at risk of demonic inversion—when they fail to leap over language but instead use it against the message itself.

When we conjure these messenger angels how do we know if we have been sent a message from the trickster Hermes or the reliable Iris? The unknown mediator's role is always ambiguous. But, to conjure encryption is to protect against the many indiscretions of the mediator. For example, signatures (hash functions) ensure authentication and data integrity, and ciphers provide information secrecy. Serres' writes:

> *"What kinds of indiscretion might be committed by an intermediary?"*
> *"If he's not happy with his brokerage fee or his tip, the courier who's carrying the gold or the silver might decide to help himself."*
> …
> *"That's why we seal letters, and put dispatches into code. We do it to protect them from indiscretions."*[61]

The message can be protected from indiscretions by putting it into code. Encryption, the process of putting plaintext into code—into ciphertext—requires *leaping over language*, and ignoring a given language's rules and particularities. Thus, cryptography is a technical aid developed to transmit language, and functions like an angel.

---

[60] Serres, *Angels, a Modern Myth*, 44.
[61] Ibid., 101.

Cryptanalysis, however, works against language. Cryptanalysis is a demonic inversion of encryption, because it betrays its mediator role. Cryptanalysis works *against* language, and against the angelic transmission from plaintext to ciphertext. Serres writes:

> *"An interpreter may actually obstruct a conversation."*
> *"Traduttore traditore, as they say. The translator as betrayer."*[62]

The translator cannot be trusted.

[62] Ibid.

9
Translation and Transcription

"Now the whole earth had one language and the same words."[1] But, brick by brick, the inhabitants of Babel built a city, and then a tower. "The Lord came down to see the city and the tower… [and said] 'Look, they are one people, and they have all one language; and this is only the beginning of what they will do…'."[2] So, the Lord scattered them about the face of the earth and confused (*Heb balal*; *confusio*) their language. So goes the story of Babel—warning humans of the sin of hubris (for building a tower "with its top in the heavens"),[3] punishing them for failing to spread across the earth and shepherd it, and giving reason to why language and things are longer isomorphic. Above all, however, Babel is the origin story of the translator.

At that precise moment, as human inhabitants spread across the earth and began to rely on translators, they also began to distrust their translators. They realized that the translator could not be trusted, precisely because the translator was a mediator. The translator sat between languages, and through error or malice, the translator also altered the message as it passed from source to destination. In fact, the very act of translation requires as much, as the craft and style of translation relies on the little parallaxes between languages and contexts. But is this always the case? Would it be possible instead, the Fallen people asked, to create a perfect, universal, and trustworthy, *machine* translator?

Since the inception of "the Babel problem," people have proposed to use cryptological resources for machine translation, a strategic alliance that still persists today. First, scholars looked around to see if any extant languages were free from the confusion at Babel, or, if corrupt, might be decoded to return them to their former purity. Several were identified as possible candidates. Hebrew was thought to contain aspects of a pre-Babel pure language, even though it existed "in a corrupted state."[4] Chinese, as inexplicable as it was to the West, was thought to be free from confusion because the Chinese did not participate in the construction of the tower, and therefore avoided God's

[1] *Genesis* 11.1. All Bible quotations are from *New Oxford Annotated Bible*.
[2] *Genesis* 11.6.
[3] *Genesis* 11.4.
[4] Conrad Gessner, quoted in Eco, *The Search for the Perfect Language*.

punishment.[5] Prior to the discovery of the Rosetta stone, it was thought that Egyptian Hieroglyphs contained the (perhaps magical) seeds of a design for a perfect language—evidence for this assertion found in the remains of the incredible accomplishments of the Egyptian society.[6]

By themselves, however, these candidate languages offered little guidance or utility for how to return to a pre-Babel purity. But, it was thought, if language was nothing but a complicated code, then code-making and code-breaking tools—cryptography and cryptanalysis—might be used to restore an impure language, or to create a pure one from scratch. That is, since antiquity, cryptography had offered a set of tools for uncovering pure prehistoric languages, for building perfect new languages, and for mediating between existing ones. Thus, there existed cryptography, as mechanical translator: perfect and therefore able to mediate with no loss of meaning or alteration (perfect isomorphism), and therefore, no more need for untrusted translators.

In this chapter I sketch some of the history and "pre-history" of mechanical translation, showing how cryptology has long been seen as a viable technology for mechanical translation. The early language planners, working in the sixteenth and seventeenth centuries, were interested in utilizing cryptological technologies for machine translation. The very earliest machines built specifically for translation were also explicitly conceived as cryptological machines. Then, by the twentieth century, a "cryptographic-translation" idea came to fruition. Following the Second World War, Warren Weaver suggested that cryptanalytical techniques could be used for machine translation, spawning modern research and development and the field machine translation.

In the years since Weaver's suggestion, references to cryptography in research on machine translation have waned, but the core principles have not necessarily changed. In this chapter, I trace these principles, from Arabic philosophers' invention of cryptanalysis over a thousand years ago, to recently declassified cryptanalysis manuals from the Second World War. Through the lens of these cryptanalysis manuals, I argue that Weaver's original suggestion highlights an important distinction often overlooked in analyses of his "cryptographic-translation" idea, namely, that cryptanalysis is conceptually (ontologically and

[5] Francis Bacon's and John Webb are two examples of scholars holding this position. In the early modern period many scholars became interested in the Chinese culture and language, in part due to a delegation of 250 men returning from China, and the translation of the 1604 work by José de Acosta, entitled *Historia Natural y Moral de las Indias*. See Lux, "'Characters Reall.'"
[6] See, for example, Athanasius Kircher's *Oedipus Aegyptiacus*. A discussion of Kircher's analysis of Egyptian Hieroglyphs and language can be found in Stolzenberg, *The Great Art of Knowing*..

methodologically) distinct from encryption and decryption.[7] Moreover, the technique of cryptanalysis, at least in a broad sense, holds promise as a viable modern technique of machine translation, whereas decryption, by necessity, does not. This is because the modern practice of cryptanalysis, having developed from statistical mathematics and sophisticated linguistics, is fundamentally a quasi-linguistic activity, and thus related to the process of translation. Here, cryptanalysis shows its true colours as a broad technique, beyond the simple sense of encryption "cracking." Cryptography, on the other hand, is a notational performance—that is, the real performance of an ideal, discrete score—a transcription, not translation, of notational symbols.[8]

9.1 History of the "cryptographic-translation" idea

The pre-history of mechanical translation originates with the early universal language planners, from the sixteenth and seventeenth centuries.[9] One of the more influential cryptographers and universal language planners was Johannes Trithemius, who developed code lists in his *Steganographia* as tools for rapidly learning Latin (his proposed solution to the Babel problem). Later, Athanasius Kircher developed Trithemius' code lists for his *Polygraphia nova*, proposing a system that would accomplish translation between languages by reducing language to its shared, essential aspects.[10] Kircher's system required that a translator look up the chosen word in a dictionary of common words (derived empirically), then construct the corresponding word by looking up in a code dictionary the semantic base along with special symbols for tense, mood, verb number, and declension. This universal, coded version could then be translated into a target language, if necessary, by reversing the process. Unlike Trithemius

[7] Terminologically, cryptography (encryption and its inverse, decryption) and cryptanalysis comprise the field of cryptology.

[8] For the introductory aspects of notation—what it is and how it relates to cryptography—see chapter five.

[9] It is fair to say that this tradition has many deep, conceptual connection to machine translation, but such a position must not be oversold. In terms of direct, historical causality (a rather too high bar for intellectual history), universal language planners do not seem to contribute to contemporary machine translation. Hutchins, a leading historian of machine translation, offers, "these [universal language] proposals must not be considered in any way as constituting embryonic automatic translation systems." Despite his dismissal of the connection, Hutchins also includes several accounts of the translation activities of universal language planners. See Hutchins, "Two Precursors of Machine Translation."

[10] For an excellent account of Kircher's role in the history of Modernity, see Stolzenberg, *The Great Art of Knowing*.

(and most other universal language planners), Kircher created several wooden "computers" for permuting through his many codes, including one that functions like an encrypting algorithm, capable of calculating a range of topics, including arithmetic, geometry, various occult symbolisms, and musical scores.[11] Kircher's wooden computers do not seem to have included natural language translation, but with their modular design, and Kircher's interests, it seems plausible that he imagined the building blocks for such a device were already available.

Other universal language planners in this era also developed methods drawn from cryptographic interests and research. For example, Francis Lodwick and Cave Beck each wrote a book on translation that was informed, perhaps in a loose sense, by the cryptographic work of Trithemius and John Wilkins (Wilkins himself published an important universal language scheme, the *Essay Towards a Real Character and a Philosophical Language*).[12] Johann Joachim Becher published a Latin vocabulary with a coded, numeric notation that, a year after its initial publication in 1661, was republished and publicized as a program for machine translation.[13] In 1661, Becher also published his *Character*, which included methods for "translating" Arabic numerals into lines and dots, a kind of encipherment that he thought deployed a more universal form of notation.[14] Francis Bacon's scientific work was also directly influenced by his cryptographic work, seeing the need to develop Real Characters that ensured direct correspondences between words and things, and by extension, the essential unification of languages.[15] In frequent discussion with cryptographers (but himself never designing such a system), John Amos Comenius had explicit political aims for his interest in universal languages, envisioning a pansophic utopia across Europe made possible only when united under one language, in a return to a pre-Babel state.

Leibniz's interest in universal languages was the beginning of the end for early language planning,[16] and bridges early modern translation schemes, such as Kircher's *Polygraphia nova,* to Leibniz's own development of analytical and calculation machines—the "machine" part of machine translation—beginning

[11] The earlier "Arca Musarithmica" is described in *Musurgia Universalis*, but Kircher's more ambitious "Organum Mathematicum," which includes music as one of many possible topics, is extant only in Gaspar Schott's *Schola Steganographica* and a few prototypes.
[12] Shumaker, *Renaissance Curiosa*, 139, 193.
[13] Hutchins, "Two Precursors of Machine Translation."
[14] See editor's introduction in Wilkins, *Mercury: Or the Secret and Swift Messenger*, xlv.
[15] Pesic, *Labyrinth*. See also chapter four.
[16] See chapter four.

with his invention of a stepped reckoner in 1673. Although the stepped reckoner could only perform simple arithmetic, Leibniz imagined an extension of the basic idea that would be capable of broad application in many fields. That is, Leibniz's proposal for a universal character (or notation), and the combinatory process of comparison and ordering (in his *Dissertatio*), were properly universal methods, in the design of his stepped reckoner.

Calculation machines following in Leibniz's footsteps became common, and developed through the well-worn historical pathways that we now associate with the history of computers: the "computers" of Babbage and Lovelace, Boole, Turing, and von Neumann. There are less familiar pathways, too, in the tradition of "mechanical brains." Rather than perform mathematical calculations (like the stepped reckoner), these mechanical brains performed logical and linguistic operations.[17] Gardner offers a series of compelling vignettes of code machines in this tradition, from Ramon Lull's thirteenth century combinatory apparatuses used to think through God's dignities, to Leibniz's universal character, to nineteenth and twentieth century machines capable of solving syllogisms (such as Stanhope's demonstrator).[18]

In addition to solving logic problems, some of these "mechanical brains" also attempted to translate between languages. The first two patents for machine translation, granted independently for G. Artsrouni and P. Trojanskij in 1933, were mechanical brains.[19] Of note, in addition to language translation, Artsrouni considered his invention particularly suitable for cryptography.[20]

Artsrouni's patent for a "mechanical brain" was broad in scope—it was really a general purpose notation ordering machine.[21] He suggested that it could be used for the automatic production of railway timetables, telephone directories, commercial telegraph codes, banking statements, and even anthropometric records (comparisons of measurements of the body), in addition to machine translation of natural languages and encryption and decryption. The machine worked by processing a series of bands containing the selected "content"—for

[17] Logic, language, and mathematics were often conflated and interrelated in the minds of these inventors, and explicitly so after Frege's project to derive the laws of mathematics from logic, later developed in Whitehead and Russell's *Principia,* at the start of the twentieth century.
[18] Gardner, *Logic Machines and Diagrams*.
[19] There is also some indication that some unknown experimenters tried to produce typewriter-translators in the early twentieth century. See Hutchins, "Two Precursors of Machine Translation."
[20] Ibid.
[21] See Ibid.; Hutchins, "Machine Translation: History." See also Mitchell, "Situation Normal, All FAHQT Up: Language, Materiality & Machine Translation," 173 ff. who draws on Hutchins' work.

the translation function this would include a target language band and a source language band; for the encryption function this would include a plaintext band and a ciphertext band. The comparison of bands was accomplished by a search mechanism, using letters input on a keyboard that would initiate the movement of the bands until a specific perforated hole on the band matched the search criteria. In this way, Artsrouni's machine was akin to the earlier Jacquard loom or the Hollerith tabulator, but with bands instead of punch cards.[22] For translation, comparison of the written materials called up by the search bands would indicate a crude word-for-word translation between the source and target languages. To be effective, the translation would work with a universal "telegraph language," an artificial language that is deliberately simplified and (as much as possible) free of ambiguity.[23] Artsrouni's machine was in fact built, at least in prototype form, and successfully demonstrated at the Paris Universal Exhibition in 1937. Orders were placed for commercial production but the Nazi occupation of France in 1940 ended any further development or deployment.

Trojanskij's patent for a mechanical translation device was a bit different from Artsrouni's, and more modest in scope. Trojanskij's machine was only intended for machine translation of natural languages (not cryptography), but, just like Artsrouni's machine it used a mechanism of moving bands to enable word-for-word translations. However, unlike Artsrouni's machine, Trojanskij's machine could code for grammatical features (working on the assumption that there are certain universal grammatical features which could be represented in "logical parsing symbols" adapted from Esperanto). Trojanskij believed that beneath language there existed precise and unambiguous relationships between words and things, which could be determined "based on scientific principles," an important component of research, reminiscent of Bacon's search for Real Characters.[24]

Although nothing immediately came of Artsrouni's and Trojanskij's proposals, following the Second World War (1946), Andrew Donald Booth and Warren Weaver discussed the possibility of machine translation (both men were unaware of Artsrouni's and Trojanskij's earlier proposals). Of the two, Weaver had the more ambitious plan, believing that fully-automatic, high-quality machine translation would be possible using cryptanalytic techniques developed during the War. Whereas, Booth believed, cautiously, that given the

[22] See chapter six for a discussion of the role of the Hollerith, or IBM, tabulator in the history of code.
[23] For comparison with Weaver's later suggestion to use Basic English for translation, see Raley, "Machine Translation and Global English."
[24] See chapter four for a description of Bacon's Real Characters.

current state of technology it would only be possible to build a mechanical multi-lingual dictionary, to be of aid to human translators. A year after Booth and Weaver's first tentative discussions, Booth and Richens worked out a "code" for mechanized dictionary translation, detailed in a Rockefeller Foundation report in 1947.[25] This preliminary work remained relatively unknown until Weaver distributed a memorandum (1949), later published with the title "Translation," to some 200 of his colleagues.[26] No doubt due to Weaver's increasing fame and power within the US (in both governmental and academic spheres), the memorandum ignited research and development of machine translation in the US and abroad. Within just a few years, research on machine translation had a dedicated journal, international conferences, and by 1955, an important collection of essays.[27]

Weaver's memorandum on machine translation starts with a curious conceit. During the War, Weaver wrote, he met an "ex-German" mathematician who had realized that it was possible to cryptanalyze a message without knowing the underlying language. Weaver recalled that during the First World War it took American cryptanalysts longer to determine the source language of an intercepted message than it did to actually cryptanalyze it. To Weaver, this suggested that language was really just a code, and that to translate from one language to another one only needed a process of decoding and recoding. Weaver wrote, "When I look at an article in Russian, I say: 'This is really written in English, but it has been coded in some strange symbols. I will now proceed to decode.'"[28] As a result of the War, powerful new tools of "decoding" were developed, in the form of successful "Bombe," Heath Robinson, and Colossus cryptanalysis machines.

In the "Translation" memorandum, Weaver offered two, somewhat incomplete, descriptions of the mechanics of his "cryptographic-translation" idea. First, he noted how the ex-German "reduced the message to a column of five digit numbers" but was unsuccessful in deriving the plaintext because the message was still "coded" in Turkish; once corrected for word spacing (and some other cosmetic changes) the original Turkish was revealed.[29] The process is never fully described, but Weaver's larger point, that language is a code, is clear enough—it's just that language is a tougher code to crack than military encryption! Second, Weaver offered a method for determining the statistical

[25] Locke and Booth, *Machine Translation of Languages*, 3.
[26] Weaver, "Translation."
[27] Locke and Booth, *Machine Translation of Languages*.
[28] Weaver, "Translation," 18.
[29] Ibid., 16.

semantic character of language, which he gave the probable value of *N*. The basic value of *N* would change according to the language to be translated, as well as the specific genre of writing, because some genres (such as the sciences) are less ambiguous, argued Weaver, and thus will have a lower probable value. For the smallest semantic unit (the word), the value of *N* could be calculated against adjacent words. Here, a particular language's grammar will dictate that *N* is not always equally distributed (i.e., "2*N* adjacent *words*"), and, that there may be a distinct value for certain parts of speech (i.e., "2*N* adjacent *nouns*").[30] Weaver's plan for machine translation seems familiar enough to a cryptanalyst: cryptanalyze using *n-gram* divisions that have been weighted on a statistical measure of letter and word frequency analysis, combined with knowledge of grammar and morphological possibilities, and *thus* you have effectively performed cryptanalysis, *or machine translation*.

This cryptanalytic process might work well for simple substitution ciphers, but Weaver realized that to do the same for two *natural* languages there was much less chance of success, since natural language contains a great deal of ambiguity and polysemy. Nonetheless, Weaver was confident that "processes, which at stated confidence levels will produce a translation which contains only X per cent 'error,' are almost surely attainable."[31] The issue at hand was, according to Weaver, "a question concerning the statistical semantic character of language."[32]

Weaver understood his "cryptographic-translation" idea to be, at a basic level, a subcategory of Shannon's Mathematic Theory of Communication (MTC), which Weaver later helped to promote.[33] In fact, Shannon himself had already made the first connection, that the study of cryptology and information were essentially related. Shannon published "A Mathematical Theory of Cryptography" in 1945 (in classified form), which detailed a logarithmic measurement of statistical information as used for cryptography, and then three years *later*, in 1948, Shannon published his famous MTC paper, reiterating and honing many of the conclusions first developed in his earlier cryptography paper. The cryptography-information connection was at the fore of Shannon's thinking, as he later noted, "the [cryptography] problem is closely related to questions of communication in the presence of noise, and the concepts of entropy and equivocation developed for the communication problem find a direct application in this part of cryptography." Again, in a retrospective 1984

[30] Ibid., 21.
[31] Ibid., 22.
[32] Ibid., 21.
[33] Weaver, "Recent Contributions to the Mathematical Theory of Communication."

interview with Ellersick, Shannon described his 1945 cryptography report as "a funny thing because it contains a lot of information theory that I had worked out before, during the five years between 1940 and 1945," and that it seemed to Shannon that "this cryptography problem was very closely related to the communications problem"[34] Despite Shannon's understanding of the close relationship between cryptography and information, Weaver's extension of Shannon's theory of information, to include the semantic properties of language, was definitely not part of the original mathematical theory of communication.

Nonetheless, in the same year that Weaver's machine translation memorandum was distributed, Weaver also published "Recent contributions to the mathematical theory of information," here stretching Shannon's cryptography-information theorem further, creating a trifecta that connected cryptography to information to translation:

> *It is an evidence of this generality that the theory contributes importantly to, and in fact is really the basic theory of* cryptography *which is, of course, a form of coding. In a similar way, the theory contributes to the problem of* translation *from one language to another, although the complete story here clearly requires consideration of meaning, as well as of* information.[35] [emphasis added]

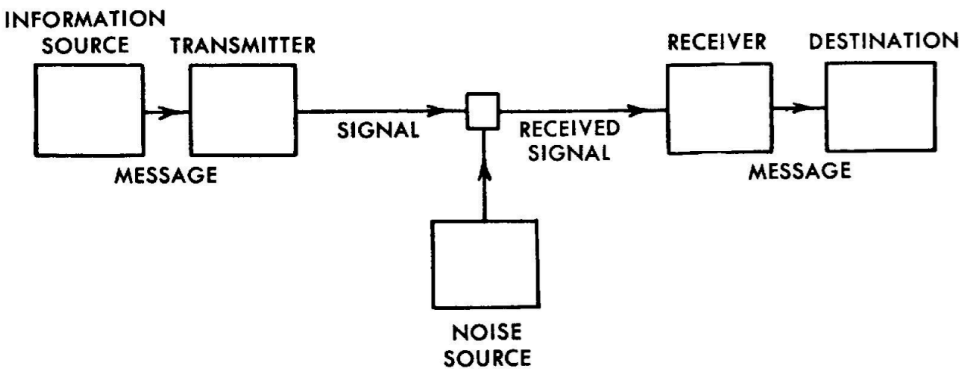
As Weaver understood Shannon's theory, the *syntactic* measurement of information that Shannon promulgated in the MTC was philosophically connected to *semantic* questions of meaning and efficacy. Most modern commentators would suggest that, in fact, Weaver deeply misunderstood Shannon's theory, but for the purposes of understanding cryptography and translation, his use of semantic considerations shines light on his otherwise opaque "cryptographic-translation" idea.

Weaver recommended Shannon's famous source-receiver diagram be amended to include a "Semantic Receiver," interposed between the "engineering receiver" (Shannon's "receiver") and the destination (Figure 9.1). Whereas Shannon's (engineering) receiver only worked on the syntactic elements of the message, Weaver's semantic receiver matched the semantics of the message to the semantic capacities of the "totality of receivers."[36] Weaver admitted that these emendations to Shannon's MTC must have seemed

[34] Ellersick, "A Conversation with Claude Shannon," 124.
[35] Weaver, "Recent Contributions to the Mathematical Theory of Communication," 14.
[36] Ibid., 15.

"disappointing and bizarre."[37] Less disappointing and bizarre, however, when we realize that Weaver clearly had in the back of his mind the "cryptographic-translation idea," hatched in the very same year, which required investigation of statistical semantics because, as any good cryptanalyst knows, the statistical semantics of natural language are not evenly distributed, and therefore can be exploited to one's advantage.

The history of cryptography is full of codes cracked because statistical semantics were deployed in cryptanalysis. For example, statistical semantics can be used to attack a weak cipher used on repetitive words, such as in salutations in letters, or other semantically "probable" words. Shannon's MTC has nothing to say about the fact that "Hello ____" is more likely to turn out to be "Hello Dolly" than it is "Hello running" (or "Hello hY!DSh;sf"),[38] but this is critical information for the cryptanalyst.[39] Likewise, a translator (machine or human) can also leverage this information, since a specific language's grammar only permits certain orderings of words for the construction of meaningful articulations. This explains why Weaver concluded his machine translation paper with a request that "statistical semantic studies should be undertaken, as a necessary preliminary step."[40]



[37] Ibid.

[38] It should be noted that the statistical measure in the MTC—entropy—is measured at the level of the smallest unit (usually a bit), not at the level of word, sentence, or larger semantic divisions.

[39] This information is only really significant when there are weaknesses in the encryption algorithm, since a very good encryption algorithm would completely obliterate this cryptanalytic possibility. Nonetheless, as recent database password hash cracking has demonstrated, small programming errors often give the cryptanalyst a toe-hold to exploit.

[40] Weaver, "Translation," 11.

Figure 9.1: Shannon's model of communication.[41]

Writing in the context of fresh memories of a devastating Second World War, Weaver wanted to adapt cryptography for peace, imagining a utopian world where the "problem of translation" ceases to affect communication between peoples, leading to a "peaceful future of the planet."[42] Like the universal language planners several hundred years prior, who sought religious and political unification with their plans for a universal language, Weaver believed that the confusion which resulted from mistranslation was a serious problem, and sought the attention of UNESCO, in particular, to back his proposal.

Weaver also realized that his proposal had limited scope—it could not, for instance, translate literary works. Nonetheless, such restrictions were acceptable for Weaver, since, according to him scientific works were more important materials for machine translation, and (Weaver imagines) being "scientific" they are less prone to ambiguity and polysemy, and therefore more likely to be adequately translated by a machine. However, one might worry, alongside Raley, that such a restriction (and product) would have the necessary consequence of instrumental rationalization, and a general diminishment of language.[43]

Following Weaver's memorandum, the field of machine translation continued to flourish, and as it developed, the strictures of intellectual camps started to form. On the one side were those researchers who, like Weaver, believed that machine translation should use statistical measure of empirical data, on the other side (basically, the linguists and philosophers), were those who thought that machine translation would need to take proper consideration of grammatical rules or underlying linguistic structures. This research proceeded until the 1960s, when Bar-Hillel produced an influential survey of the field of machine translation and concluded that, not only was the prospect of fully-automatic high-quality translation unrealistic given the current state of technology, but that the entire project was impossible in principle.[44] In 1964, government sponsors (mainly military and intelligence agencies—already familiar with cryptological resources) asked the National Science Foundation to examine the apparently slow development of machine translation. The resulting report was critical, arguing that machine translation was slower, less accurate,

[41] Weaver, "Recent Contributions to the Mathematical Theory of Communication," 4.
[42] Weaver, "Translation," 18.
[43] Raley, "Machine Translation and Global English," 307.
[44] Hutchins, "Machine Translation: History," 375.

and twice as expensive as human translators. According to Hutchins, this report basically killed research on machine translation in the US for the next few decades (although research continued, to a limited degree, elsewhere).[45]

After a number of years, machine translation research began to pick up, and by the 1980s, machine translation was proving successful and starting to find commercial application. New methods and models improved the quality of translation, and the introduction of faster and cheaper microcomputers spurred further success while continuing to drive costs down. In the 1990s, research moved away from rationalist programmes that had sought to understand underlying linguistic rules, and returned to the empiricism Weaver first imagined, using large language corpora and sophisticated statistics. One important system during this transitional time was Candide, developed by IBM, which used frequency statistics as applied to a corpus of Canadian French and English parliamentary debates.[46] In recent years Google has similarly leveraged its vast stores of linguistic data, collected from the web, and its expertise in computational language processing, to create a product that is considered to be market leading. Google's approach to machine translation vindicates Weaver's basic intuition, since Google has openly declared that they do not employ linguists,[47] even going so far as to create inter-language dictionaries programmatically, rather than by relying on human-created ones.[48]

9.2 Language and cryptanalysis

Weaver's description of his "cryptographic-translation" idea rested on the success of Allied cryptanalysis during the Second World War, however, Weaver does not fully explain this process, either for fear of disclosing sensitive classified information or simply out of ignorance to how such a process might work. Thankfully, we are now in a position to better understand what Weaver might have intended. In 2005, the National Security Agency (NSA) declassified a trove of materials written by their celebrated chief cryptologist, William Friedman (1891–1969).[49] After his groundbreaking "The Index of Coincidence" cryptanalysis manual (lauded by historian of cryptography, David Kahn, as the "most important single publication in cryptography"),[50] written during the

[45] Ibid., 376.
[46] Ibid., 380.
[47] Schulz, "Translate This."
[48] Kelly, "Why Machines Alone Cannot Solve the World's Translation Problem."
[49] Friedman became chief cryptologist in 1952, upon the formation of the NSA.
[50] Kahn, *The Codebreakers*, 167.

interbellum (first proposed in 1920, then published in 1922),[51] Friedman went on to produce several training manuals that rationalized extant cryptanalytic techniques and further expounded on his statistical coincidence techniques. As a set of training manuals, the techniques described in the *Military Cryptanalysis* series cannot be considered "cutting edge" for the time,[52] but they do offer insight into the kinds of cryptanalysis Weaver might have been exposed to in his bureaucratic and scientific work, and therefore help to illuminate his "cryptographic-translation" idea.

Before comparing Friedman's methods to Weaver's proposal, however, I will first dig deep into the past, to describe the origins of many of the principles laid out in the *Military Cryptanalysis* series, which were in fact discovered by Arabic philosophers[53] over a millennium ago. These resources highlight two important points: 1) the methods and ontology of cryptanalysis are closely aligned with language (and therefore, distinct from encryption and decryption); and 2) since its inception, cryptanalysis has been historically co-determined by language and the study of language, and thus emerged as a surprisingly natural fit for machine translation, ultimately vindicating Weaver's suggestion.

9.2.1 Invention of cryptanalysis

In David Kahn's history of cryptology, he states that "cryptology was born among the Arabs," and that "they were the first to discover and write down the methods of cryptanalysis."[54] When Kahn was writing *The Codebreakers* in the 1960s, the oldest known work on cryptanalysis was al-Qalqasandi's *Subh al-'a'sa* from 1412, which paraphrased ibn ad-Durayhim's work from a century prior. In the 1980s, a number of new cryptological manuscripts were discovered in the as-Sulaymaniyya Library in Istanbul, dramatically rewriting the history of

[51] Later republished as Friedman, *The Index of Coincidence and Its Applications in Cryptanalysis*.
[52] For a description of the cutting edge of cryptanalysis at this time, see Diffie, Reeds, and Field, *Breaking Teleprinter Ciphers at Bletchley Park*.
[53] In this complex era of military, cultural, and intellectual expansion, beginning shortly after Mohammed's founding of Islam until around the thirteenth century (or later), and covering a massive range of disciplines, not all philosophers were ethnically Arab, and nor did they all speak and write in Arabic. Many important philosophers lived in Andalusia, Spain, or deep into Africa, and discoursed in Latin, Hebrew, and the many vernaculars encountered during the Islamic Empire's rapid imperialist expansion. Thus, there is no good catchall term for these peoples, but following Gutas, I refer to "Arabic" philosophers because they were united in their relationship to Islam and the socio-economics of the Caliphate, which operated in Arabic. See Gutas, "The Study of Arabic Philosophy in the Twentieth Century."
[54] Kahn, *The Codebreakers*, 80.

cryptography.[55] Among these manuscripts was al-Kindi's *Risala fi 'istikhrag al-mu'amma*,[56] written in the ninth century, over five hundred years before al-Qalqasandi's work, and even longer before Leon Battista Alberti's work, which introduced the systematic study of cryptography and cryptanalysis to the West.[57] Al-Kindi's work is the oldest extant work on cryptography and cryptanalysis, although there are references to even earlier Arabic works, dating to the early eighth century.[58] Of the Arabic writings on cryptology that followed, nearly all draw from al-Kindi, who set out the essential aspects of cryptography and cryptanalysis.

The Arabic cryptographers had very detailed and highly developed terminology, and precise analytical distinctions for the field of cryptology. The principle distinction between encryption ("*at-ta'miya*")[59] and cryptanalysis ("*at-targama*" and "*istihrag al-mu'amma*") was typically maintained, although the latter sometimes stood in for the entire field, what we now call "cryptology" (the encompassing field of cryptography *and* cryptanalysis). Likewise, the Arabic cryptographers had words for basically all modern distinctions: plaintext, ciphertext, nulls, code, keys, steganography, *n*-grams, and so on.[60] It is quite telling that Arabic cryptologists maintained such a division between cryptography and cryptanalysis, although the terms used to represent the concepts were themselves quite fluid. Cryptanalysis (*istihrag al-mu'amma*) was considered the process of converting ciphertext into plaintext without the use of a key, which was sometimes also called "interpretation" (*at-targama*),[61] which also meant "translation"—a reference to the semiotic transformations of natural language. The process of enciphering (or encrypting), on the other hand, was considered a distinct process that involved the reordering and substitution of

[55] These first works were edited and published in Arabic in 1989 by a group of scholars in Damascus. Since 2003 they have re-published the earliest works in a new series, alongside other recently discovered works, now totalling six volumes available in edited Arabic versions with English translation. Despite the significance of this work, the impact has been limited, both inside and outside the history of cryptography. See Al-Kadi, "Origins of Cryptology"; Schwartz, "Charting Arabic Cryptology's Evolution"; Schwartz, "From Text to Technological Context."
[56] Mrayati, Yahya, and Hassan, *Al-Kindi's Treatise of Cryptanalysis*.
[57] Prior to Alberti, in the West, cryptography was in ample use for millennia, but seemingly never systematized. See, e.g., Kelly, "The Myth of the Skytale." for a re-evaluation of the ancient's use of an encrypting device called the *skytale*, and King, *The Ciphers of the Monks*. for a description of some of the ciphers used during the Middle Ages.
[58] Mrayati, Yahya, and Hassan, *Al-Kindi's Treatise of Cryptanalysis*, 39.
[59] The English term "cipher" actually originates from a Latin version of the Arabic *sifr*, meaning zero. See Ibid., 24.
[60] Ibid., 24–32.
[61] Ibid., 24.

letters (al-Kindi's description of what is now called monoalphabetic encryption is highly sophisticated and original, utilizing all manner of syntactic arrangement, from bigram substitution, to transposition, to the use of codes and symbols).

Al-Kindi's methods of cryptanalysis involved three distinct processes that could be used together, and as well, he provided suggestions specific to cryptanalysis of poetry (a common issue for Arabic cryptanalysts). The first process uses letter frequencies, both for cryptanalysis and for determining the underlying language of a ciphertext (recall Weaver's admission that the Allies often found it more difficult to determine the source language of an encrypted message than it was to cryptanalyze). Al-Kindi called this process "the quantitative [*kammiyya*] expedients of letters," which "include determining the most frequently occurring letters in the language in which cryptograms are to be cryptanalysed."[62] This process tabulated the letter frequencies of the ciphertext (ensuring that the ciphertext was of a sufficient, that is, statistically-significant, size, al-Kindi noted) and then compared that distribution against the letter frequency distribution of a plaintext corpora (and ideally one of the same genre, since, for example, poetry would have a different distribution).[63] In the process of comparison, al-Kindi wrote, "we mark the most frequent letter 'first', the second most frequent 'second'," and so on, and in the distribution for our plaintext corpora we search "for the most frequent symbol… and regard it as being the same letter we have marked 'first'… ."[64] To aid the reader, al-Kindi produced tables of letter frequencies for Arabic (Figure 9.2), the first ever such exercise, which would eventually become a vital practice for early statistics and those fields that depend on these kinds of calculations.[65]

[62] Ibid., 122.
[63] Al-Kindi is implicitly aware of the differences between letter frequency distributions in various genres or styles, but the notion is never followed up on. It was Alberti, in his *De Componendis Cifris* (1467), who made the first ever explicit "stylometric" observations. See Alberti, "De Componendis Cifris"; Ycart, "Letter Counting"; Ycart, "Alberti's Letter Counts."
[64] Mrayati, Yahya, and Hassan, *Al-Kindi's Treatise of Cryptanalysis*, 123.
[65] The first Western cryptology manual to give letter frequency tables was Charles François Vesin de Romanini in the mid-nineteenth century. The practice of producing and using letter frequency tables was considered by Babbage and Quetelet to be one of the "constants of nature and arts," and of critical value to printers who would need to ensure sufficient quantities of metal type were ordered. Samuel Morse utilized the letter frequency values of the printer's cases when determining efficiencies for his binary telegraph code. See Ycart, "Letter Counting," 307, 312.

Letters	Frequency	Letters	Frequency	Letters	Frequency	Letters	Frequency
ā (ا)	600	n (ن)	221	k (ك)	112	ḏ (ذ)	35
l (ل)	437	r (ر)	155	d (د)	92	ṣ (ص)	32
m (م)	320	ʿ (ع)	131	s (س)	91	ḫ (خ)	20
h (ه)	273	f (ف)	122	q (ق)	63	ṯ (ث)	17
(*) ū+w (و)	262	t (ت)	120	ḥ (ح)	57	ṭ (ط)	15
(*) ī+y (ي)	252	b (ب)	112	ǧ (ج)	46	ḡ (غ)	15
						ẓ (ظ)	8

Figure 9.2: Reproduction of al-Kindi's letter frequency table.[66]

Al-Kindi's frequency analysis process was effective at revealing a probable plaintext from ciphertext, but it could also help determine what language any given text might be "encoded" in. As al-Kindi explained, "certain languages… [have] vowels… greater in number than some other vowels, while non-vowels [i.e., consonants] may be frequent or scarce according to their usage in each language, such as the letter s, of which frequency of occurrence is high in Latin."[67] Al-Kindi thus identified how the vowel-consonant ratio is highly dependent on the specific language, and also style. Although al-Kindi never extended his analysis, there is evidence, following Bernard Ycart's exposition, that al-Kindi's early explorations of vowel-consonant ratios anticipated computational linguistics, including authorship attribution questions and machine translation.[68]

Al-Kindi's second process for cryptanalysis was based on linguistic rules, specifically morphology and word derivations (falling under the science of the "laws of single words"), which he called "qualitative [*kayfiyya*] expedients." Al-Kindi's deep knowledge of Arabic enabled him to describe the many "combinable" and "non-combinable" letters and their valid orders and positions.[69] With knowledge of these morphological forms, a cryptanalyst (or translator) would be able to reduce the number of valid letter positions, which, when combined with letter frequency statistics could be very useful for cryptanalysis, especially for transposition ciphers. Later, ibn ʿAdlan (1187-1268)

[66] Mrayati, Yahya, and Hassan, *Al-Kindi's Treatise of Cryptanalysis*, 168.
[67] Ibid., 122.
[68] Ycart, "Letter Counting," 314.
[69] Mrayati, Yahya, and Hassan, *Al-Kindi's Treatise of Cryptanalysis*, 172 ff.

built on al-Kindi's approach, analyzing valid word formations from *n*-gram combinations by starting with bigrams and trigrams compared against a dictionary of words to determine which combinations of letters form actual words.[70]

The third process of cryptanalysis described by al-Kindi was based on the semantic properties of actual texts, called the "probable word" method. Al-Kindi described how common words or phrases, such as the common opening for Islamic works, "In the name of God, the Compassionate, the Merciful," can be used "as a guide throughout the cryptogram."[71] Al-Kindi did not spell out the "probable word" method, but the idea is simple enough—if a cryptanalyst can detect that some ciphertext may correspond to a certain common or probable word, guesses can be made as to what plaintext letters might correspond to the ciphertext letters, which may reveal a key or common substitution used throughout the ciphertext. Additionally, Al-Kindi recommended that the cryptanalyst ought to be aware of the fact that genres and styles may have particular phrases and probable words, which should be leveraged for cryptanalysis as appropriate.[72]

Arabic philosophers were accomplished cryptologists for a variety of reasons. Skill in mathematics, including the development of a highly useful numeral notation (which the West adopted),[73] was an essential component to understanding letter frequency statistics, and a well-developed administration and tradition of academics helped sustain research, while providing many reasons and motivations for the practical application of cryptography and cryptanalysis (in statecraft and poetry, alike).[74] Above all, perhaps, skill in Arabic linguistics that developed as part of a critical apparatus of Quranic interpretation and the production of literature, in combination with a very important translation tradition, were critical causes for proficiency in cryptanalysis. Aside from these important social structurations, Arabic philosophers also believed that language was sacred, powerful, and, just as Weaver supposed, coded. For example, at the end of the Arabic "golden age," ibn Khaldun (1332-1406) argued that words were veils, working to conceal yet reveal the links between thought and understanding.[75] Humans could not

[70] Mrayati, Yahya, and Hassan, *Ibn `Adlan's Treatise Al-Mu'allaf Lil-Malik al'Asraf*.
[71] Mrayati, Yahya, and Hassan, *Al-Kindi's Treatise of Cryptanalysis*, 128.
[72] Ibid.
[73] See chapter five for the later development of mathematical notation in the West.
[74] It has also been argued that papermaking skill was an important factor in the development of Arabic cryptology, see Schwartz, "From Text to Technological Context."
[75] Cooke, "Ibn Khaldun and Language," 180.

escape language—the "Babel problem"—but, ibn Khaldun thought, humankind's "greatest power and gift" was communication,[76] and so, as long as some people were sufficiently trained, and naturally smart and hard-working, the veil of language could be lifted.

This brief description of early cryptanalysis only hints at its complexity and long history—a history not yet written, and a project only recently possible due to the discovery (and subsequent English translations) of important Arabic resources. Despite the historiographical challenges, this history reveals that, as Kahn stated so many years ago, cryptanalysis was born with the Arabs. In the West, following Arab developments, but seemingly independent of the extensive development by Arabic philosophers, systematic cryptanalysis originated with Alberti in the fifteenth century. Cryptanalysis then continued in state and Papal offices throughout the centuries (resulting in numerous "Black Chambers"), making greater strides in quantity of cryptanalytic work than in quality of cryptanalytic research. During late modernity, research on cryptanalysis again intersected with emerging statistical techniques. By the early twentieth century, knowledge of language and statistics far outpaced research in cryptanalysis, and research flowed from the outside to the inside, with few cryptological contributions impacting other fields, until Shannon's theorizations of information in the late 1940s, which was (as noted above) directly inspired by his research on cryptography.

9.2.2 Early twentieth century cryptanalysis

The deep ties to rules, behaviors, and styles of natural language, and its translation, which were present at the inception of cryptanalytic research, remained well into the twentieth century.[77] The use of statistical measures for cryptanalysis was inherited from the Arabs, and used equally on ciphertext and natural language corpora. In fact, the medieval Arabic philosophers would not have seen Weaver's suggestion for a "cryptographic-translation" idea as foreign or misguided (insisting, however, that Weaver really meant "*cryptanalysis*-translation"). Nonetheless, to gain a little more purchase on what Weaver meant by his opaque notion of translation, I introduce an example of early

[76] Ibid.

[77] The recent development of extremely robust encryption algorithms that utilize a massive combinatory space, made possible by computerization, have in recent years caused practical cryptanalysis to lose many of its ties to language. A variety of "probable word" cryptanalysis still exists for password cracking, as hashed passwords can be guessed by dictionary-style attacks, but for most other forms of cryptanalysis the erasure of linguistic traces is so complete that purely linguistic approaches are effectively rendered useless.

twentieth century cryptanalysis, in the form of Friedman's *Military Cryptanalysis* series of manuals. While the state of the art had certainly developed over the millennium separating al-Kindi and Friedman, many of the basic principles from the former are still present in the latter, including references to language translation of the sort Weaver might have had in mind.

Friedman's *Military Cryptanalysis* series contains four volumes of ascending difficulty and utility, published between 1938 and 1941. The first volume lays the groundwork, starting with simple monoalphabetic ciphers and the letter frequency distribution method of cryptanalysis, identical in its essential aspects to al-Kindi's work. The latter volumes tackle newer polyalphabetic ciphers and more advanced methods of cryptanalysis, covering material that has no strict historical connection to Al-Kindi or early Arabic cryptanalysis. Polyalphabetic encryption, for example, was unknown to the Arabic cryptologists, since it was invented in the West by Alberti, described in his *De Cifris* (1467).[78] Nonetheless, despite its more recent vintage, the simpler letter frequency approaches developed in the Middle Ages are still of value for polyalphabetic cryptanalysis—as Friedman described it, cryptanalyzing polyalphabetic ciphertext requires reducing the "complex, heterogeneous, polyalphabetic text to simple, homogenous, monoalphabetic text," which is ultimately cryptanalyzed using the traditional methods.[79]

Friedman provided a list of the four basic operations of cryptanalysis: 1) the determination of the language employed in the plaintext version, 2) the determination of the general system of cryptography employed, 3) the reconstruction of a key or code book, and 4) the reconstruction or establishment of the plaintext.[80] The first step is critical, and highlights the degree of overlap between cryptanalysis and language translation.

To determine the language employed in the plaintext version, Friedman recommended that the cryptanalyst could often make an educated guess, based on prior knowledge about the origins of the ciphertext message. But, in some cases, the message sender may use an unexpected language as subterfuge, as when, e.g., the Germans would occasionally write in English during the First World War.[81] A better approach, Friedman offered (echoing al-Kindi's method for determining the message's language), was to use the fact that, "in special cases," a "clue to the language employed is found in the nature and composition

[78] See chapter three for the history of Alberti's development of polyalphabetic encryption.
[79] Friedman, *Military Cryptanalysis: Part III Simpler Varieties of Aperiodic Substitution Systems*, 73.
[80] Friedman, *Military Cryptanalysis: Part I Monoalphabetic Substitution Systems*, 7.
[81] Ibid.

of the cryptographic text itself."[82] Friedman pointed out that certain languages do not contain, or rarely use, certain letters (Friedman cited the lack of letters K and W for Spanish, similarly, al-Kindi offered that the letter S occurs in abundance in Latin). Other unique linguistic features may also help the cryptanalyst determine the language, Friedman continued, such as special bigraphs (CH in German), or regionally-specific eccentricities (Japanese Morse code contained unique combinations).[83] Knowledge of these special characteristics of language were important aspects of successful cryptanalysis.

Friedman also suggested that in some cases cryptanalysis could proceed without knowing the underlying language, especially in "frequency studies." Just as in Weaver's story of the "ex-German," Friedman noted that "analytical processes" may be performed without knowledge of the language, and "by a cryptanalyst wholly unfamiliar with the language even if it has been identified, or who knows only enough about the language to enable him to recognize valid combinations of letter, syllables, or a few common words in that language."[84] These cryptanalytic "solutions" from cryptanalysts ignorant of the source language, however, are not really solutions, Friedman noted—rather "such a 'solution' calls for nothing more arduous than the ability to recognize pronounceable combinations of vowels and consonants—an ability that hardly deserves to be rated as 'cryptanalytic' in any real sense."[85] Thus, the cryptanalyst invariably benefits from the assistance of a translator—"cooperation between cryptanalyst and translator," writes Friedman, "results in solution."[86]

The "frequency studies" Friedman described are basically identical in kind to those described by al-Kindi. Friedman demonstrated that across single language corpora, the "uniliteral" (single-letter) frequency distribution will remain "constant" within a "characteristic frequency" distribution, depending on the length of the text analyzed (Friedman provided charts for the expected amount of deviation in a message of a given length).[87] It is also possible to extend this analysis to biliteral distributions. For short texts there may be considerable variance, especially if the two texts are from different styles (such as telegraph messages, or messages from specific commercial sectors, in comparison to, say, prose or poetry), but as the length of the text increases the "agreement, or

[82] Ibid., 8.
[83] Ibid.
[84] Ibid.
[85] Ibid.
[86] Ibid.
[87] Ibid., 12, 20.

similarity, would be practically complete" (emphasis in original).[88] Similarly, the vowel-consonant ratio is characteristic and reasonably stable across a single language.[89] Friedman cautioned that such similarities are "statistical generalizations" and may not always hold, but that "nevertheless the normal frequency distribution… for any alphabetic language is… the best guide to, and the usual basis for, the solution of cryptograms of a certain type."[90]

Comparison of ciphertext and expected letter frequency distributions may occur in a variety of ways. For pure transposition ciphers, the letter frequency distribution tables can be visually inspected and shifted by hand, lining up the crests and troughs (Figure 9.3). Such a procedure, Friedman noted, must progress with caution, as assumed fit may be "pure coincidence" or the result of "something more than simple monoalphabetic substitution."[91] Deviation from the expected distribution might be evidence that a more complex cipher was used, or that the message was written in a language other than the one it is being compared against. This basic procedure can also be used to test bi- and trigrams, and especially diphthongs or other morphological markers, such as the "tetragraph [tetragram] of considerable importance in English, *viz*, TION [as in the English word "examina*tion*"],"[92] or the "succession of three vowels [which] are rather unusual in English."[93]

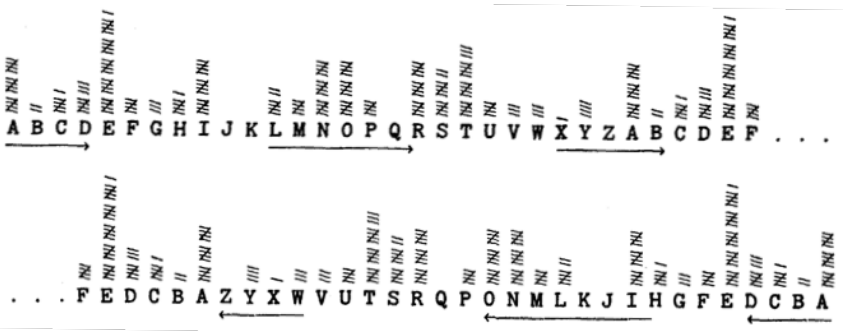


Figure 9.3: Friedman's comparison of uniliteral frequency distribution tables.[94]

[88] Ibid., 12.
[89] Ibid., 14.
[90] Ibid., 16.
[91] Ibid., 28.
[92] Ibid., 49.
[93] Ibid., 54.
[94] Ibid., 28.

The three following volumes build on Friedman's "index of coincidences" method, first published in 1922 but rewritten for the *Military Cryptanalysis* series as an appendix. This method distinguishes itself from some other methods that rely on intuition, Friedman argues, because it deals with the "phenomena of repetition[,]… statistically."[95] These statistical measures are necessary for a programme of scientific cryptanalysis. For example, Friedman demonstrated that a "uniliteral frequency distribution of a large volume of random text will be 'flat,' i.e., lacking crests and troughs."[96] In an English text corpora, on the other hand, the probability of any given letter is 0.0385, that is, it can be expected a given letter will occur about 3,850 times in a corpora of 100,000 letters.[97] For a corpora of random text, however, the frequency of letters follows different, but specific, statistical curves, namely "Poisson's exponential expansion," or the "law of small probability curves." Such curves can also be determined for "other types of texts."[98] Determining the "index of coincidence" is statistically more sophisticated than anything required for simple frequency studies, but the processes are essentially the same.

Cryptanalysis certainly appears to be connected to machine translation at a number of points, and it is likely a useful connection too, but whether we want to actually call the cryptanalytic process "translation" is another, more difficult question. While not answering this question here (first requiring an answer to what translation is itself), I have shown how cryptanalysis often makes use of statistical semantic properties, ought to be aware of the differences of style and content of corpora, and ultimately results in, at best, an underdetermined probability. Arguably, all effective human discourse requires some attention to these kinds of issues, but machine translation, in particular, functions principally by these very processes.

One question remains: if *cryptanalysis* is fundamentally a process that works *with* language, in what way does *encryption* relate to language? As I demonstrate, encryption and decryption are not forms of translation, but rather, they are forms of transcription.

[95] Friedman, *Military Cryptanalysis: Part II Simpler Varieties of Polyaphabetic Substitution Systems*, 108.
[96] Ibid.
[97] Ibid., 109.
[98] Ibid., 112.

9.3 Transcription and the encryption performance

There are three parts to a complete cryptographic system, and they are conventionally termed plaintext, encryption (/decryption), and ciphertext. This chapter has been concerned with the mediatic middle—encryption—and how it relates to language. I described how cryptanalysis works on natural language itself, with methods requiring attention to linguistic rules and actual linguistic behaviours in the form of text corpora. I showed that, in this way, cryptanalysis is related to, and provides a sensible model for, machine translation.

The case is very different for encryption and decryption. Before something can be encrypted it must first be rendered into plaintext, which is a special kind of notational inscription that *may* be token-identical to typical alphabetic writing (including some unusual "coded" forms too), but also excludes many other forms of expression.[99] Plaintext is distinguished from other token-identical forms of writing because it is a vector pointing towards encryption, that is, plaintext is suitably-prepared writing that *can be* encrypted. The distinction between, say, alphabetic writing and plaintext is, on many levels, a distinction without difference—but the distinction is critical nonetheless. The distinction is critical because, given the representational violence in the process of creating notation (see chapter three), the creation of plaintext is not innocent. Indeed, writing, in the first instance, is not innocent.[100] But, by relying on the processes involved in creating plaintext, encryption adds further properties that are nonetheless problematic. By maintaining the word "plaintext," as opposed to mere "alphabetic writing" (and other codes), we can identify, and hold accountable, the encryption processes that perform these additional actions.

Encryption (and its reverse, decryption) works by establishing a mutually determining "semantic" link between plaintext and ciphertext—origin and destination. This link determines a "machine representation" that precisely "picks out" a specific piece of notation (a "unity" in Leibnizian terminology)

[99] See chapter five for a full discussion of notation. The issue is not whether some things can or cannot be represented in plaintext—the issue is whether we would want to represent it as plaintext, or be willing to accept the representation. To use the example from chapter five, a painting qua painting cannot (typically) be considered notational.

[100] The very act of representation, and of (machine and human) thinking, involves a great deal of violence—some of which may be acceptable, while some is not. Consider, for example, hate speech, or credit scoring algorithms. Moreover, perhaps some things should not be represented at all? Or, similarly, perhaps some things should not be encrypted?

from within the combinatory space of ciphertext. The resulting ciphertext must also be determinate of, and determined by, the encryption system. This process is a form of "transcription" as opposed to "translation" because it transforms the origin to destination according to internally-sourced semantic rules (the encryption algorithm), as opposed to externally-sourced semantic rules (the grammar associated with the source or target language). Therefore, transcription is a semantic exchange (as I described in chapter five), but not in the way we normally understand semantics.

Consider, again, the ways that the same description of encryption can be stated in language more familiar to Goodman's theory of notation. Unlike many other kinds of representational shift, the process of encryption tightly binds plaintext to ciphertext by determining a "compliance class" that precisely denotes one notational mark from the plaintext to another notational mark from the combinatory space of ciphertext. The doubling of encryption extends the notational properties of plaintext further out, from syntax to semantics. The notational criteria of disjointedness and finite differentiatedness then take on semantic valences, to which the criterion of unambiguity is added (resulting in what Goodman called a "notational system").[101] In the simple example of a transposition cipher, when the doubling of <r> within a notational *system* (syntactic and semantic requirements) establishes <r> as is a compliant of its double <q>, the system is described by the syntactic transposition <r>-<q> and the associated semantic rules (in this case the rules might be "move the index letter one position to the right," but more realistic examples use more complex algorithms).

For comparison, the transcription process of encryption can also be understood as a "performance," in exactly the same way that a musical score is performed. In music, there is a widely accepted notational system for "writing down" musical performances (since about the eleventh century, musical notation uses marks indicating specific pitches on a five-line staff, related to medieval "neumes"). The marks involved in musical notation are syntactically disjoint and finitely differentiated, and therefore constitute a notational scheme.[102] Moreover, the set of marks called a musical score is syntactically and *semantically* disjoint and finitely differentiated, and unambiguous because each written note represents a (potentially) *performed note*, and the performed note is

[101] Goodman, *Languages of Art*, 148. Note that ambiguity occurs when any character has different compliants at different times or in different contexts. For unambiguous systems, syntactic equivalence (disjoint and differentiated) implies semantic equivalence.
[102] See chapter five for a description of the criteria of notational schemes.

also determinately represented by the written one (in order to count as part of the notational system).[103] The whole musical score serves to determine the compliance class of performances.

By consulting the score during a performance one can determine if the performance is Beethoven's 9^{th} *Symphony* or Bach's *Goldberg Variations*, or something else entirely. Only those performances that hit the correct keys in the correct order (within some degree of practical tolerance) get to be called the 9^{th} or the *Goldberg Variations*. The score itself is a kind of abstraction, since it does not matter *in terms of the compliance class* if the performance occurs on a rainy day, on an electric keyboard, or if the score itself is a rough photocopy—so long as the correct notes are played. Similarly, if the musicians playing the 9^{th} decide to add some improvisation, through error, choice, or malice, the performance is not strictly-speaking the 9^{th} any more, it is a performance of a new work—derivative of the 9^{th}, but distinct.

Encryption is also a performance.[104] The notational plaintext is equivalent to the set of musical notes, comprised of syntactically disjoint and finitely differentiated marks. Together, the notational plaintext *and the specific encryption algorithm* are equivalent to the musical *score*. Encryption takes notational plaintext, and mark by mark "performs" the transcription to establish a semantic link between plaintext and ciphertext. For example, in the same way that a notated (middle) "C" is semantically linked to the sound emitted from a piano at a specified vibrational frequency (261.63Hz) (the "note C" *means* "sound expressed at 261.63Hz"), <r> is transcribed to <q> through encryption according to some specified algorithm (figure 9.4 depicts this parallel between musical performance and encryption performance).

[103] In actual use, musical notes have a great deal of ambiguity and therefore rarely work precisely as notations. However, as per Goodman's analysis, musical notes *should* be a proper notation system.

[104] In chapter five I also discuss encryption in terms of performance, noting that as an allographic (not autographic) art, the performance of encryption links semantic entities. Recall that allographic arts are comprised on constitutive notational elements, which ignores the fact that any given performance may have many contingent properties (such as being aesthetically beautiful).

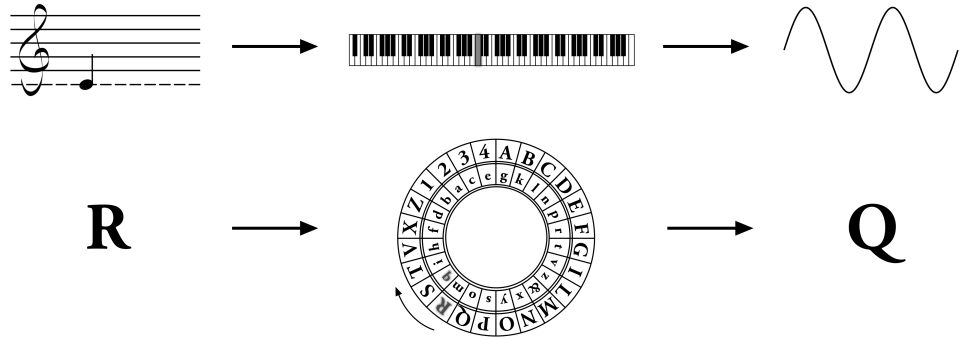


Figure 9.4: A diagrammatic depiction of the parallel between musical performance and encryption performance.

Unlike musical performance, encryption is typically thought to provide secrecy and security, but these are social properties of encryption, and in fact, not unique to the types of notation we typically associate with encryption. When used for secrecy and security, complexity is often part of the encryption performance. However, encryption is not the only complex form of notation possible. Binary encoding is also a (somewhat) complex form of notational transcription, or "encryption." So is the form of performance art known as "Black MIDI," which attempts to create music that is so highly complex the notational representation is "black" (and, it should be noted, the music can only be played by a machine). The complex result if superficially similar to ciphertext (see Figures 9.5 and 9.6).

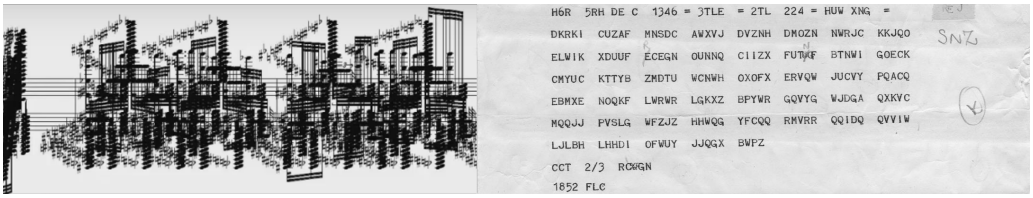


Figure 9.5: Comparison of complex notation: black MIDI; and Figure 9.6 (possibly Enigma) encrypted text.[105]

But, complexity is not the only test for encryption. There are in fact a great number of edge cases, even linguistic ones, that appear from some perspectives to be complex and "secret," but from different perspectives appear simple and not secret at all. For instance, upon first hearing Pig Latin a child believes the cipher is good—private communication among confidantes! Quickly, however, the simple transposition encryption rules are cracked, and with a little practice

[105] Trobsky, *Español*; Lord, "Enigma Decrypts."

rules can be performed on the fly, as though a kind of pidgin language has been constructed. Similarly, some people who have great command over the internal processes of computers are capable of "reading" and "writing" machine code, or perhaps even binary code itself. Do Pig Latin and machine code count as natural languages, artificial languages, or as encryption ciphers? Pig Latin and machine code probably do not have enough linguistic markers to be called natural language, but at what point of complexity (or similarity to natural language) does a system cease to be a pidgin, an artificial language, or an encryption cipher, and start to become a "real" language? When does a weak cipher cease to be a cipher at all? There is no essential division between these forms of complex representation.

The double demand of encryption—an encryption system uniquely *determining* a ciphertext, and an encryption system uniquely *determined by* a ciphertext—is a high bar for notational systems like encryption. The requirement is a necessary one, however, because cryptography is *special* precisely because it is able to situate a tiny bit of information within a much larger combinatory space, and therefore if any ambiguity were introduced, the system would lose hold of this tiny bit of information within the sea of seemingly entropic chaos (which, however, is actually highly ordered notation with the appearance of entropy). Such a loss would make the original plaintext unrecoverable, making cryptography not perfect and ideal, but instead merely probable—therefore, reducing encryption to cryptanalysis, and notational plaintext to natural language text. Such a loss obviates the point of cryptography, and renders the category of expression empty.

❦

It is often claimed that cryptanalysis is merely decryption by another means—a way of getting around the inconvenient fact that you may sometimes be without the correct key. I have shown that, in fact, cryptanalysis and cryptography have very different methods, and distinct, non-commensurate ontologies, in the sense that ontology is understood as being disclosed in history (but with blurred lines in practice). Stemming from medieval Arabic statistical methods, cryptanalysis is necessarily linguistic, utilizing semantic and probabilistic features of language, which shares a lineage with machine translation. Encryption, on the other hand, is a special kind of notational performance; a form of ideal machine writing, distinct from language, and having more in common with other notational technologies, such as musical scores and their performances. In this way, if my interpretation of Weaver's proposal for machine translation as a "*cryptanalysis*-translation" idea is correct, then, he was

right to reimagine the field of machine translation in terms of statistical semantics. Progress in modern machine translation, it seems, has vindicated this approach.

In the end, George Steiner writes, "not everything can be translated."[106] Limits are set by theology and gnosis, suggesting that "there are mysteries which can only be transcribed… in such cases it is best to preserve the incomprehensible."[107] For these cases, cryptography presents a technological answer for things that cannot or should not be translated.

[106] Steiner, *After Babel*, 406.
[107] Ibid.

Part 3: Ciphertext

In this part I rewrite the term "ciphertext." Chapter ten describes ciphertext in terms of Otherness and order, offering historical comparisons with early calculating machines and the scientific study of order; I also present a case study of Andrés Ramírez Gaviria's new media art that interrogates the many ways that the Otherness of ciphertext can be exposed. Chapter eleven revisits the history of the Spartan skytale to show how silence is a property of ciphertext, and also analyses the properties of silence to show how ciphertext is a positive deconstruction of language, sometimes even making a farce out of speech.

10
Otherness and order

Ciphertext is the last step in a complex process. Because notational plaintext is transmitted and transcribed, rather generically, as encryption, any number of functions and uses can be imagined. This is part of the reason why cryptography has been so astonishingly powerful and ubiquitous in a world already filled with code.

In this chapter I discuss the ways that ciphertext orders and is ordered, the results of which can also be aesthetic. To demonstrate these potential aesthetic elements, I explore the work of new media artist Andrés Ramírez Gaviria. An important feature of Gaviria's work is that he is able to demonstrate and exemplify the aesthetics of ciphertext as something foreign—as "other"—sitting "Between Forms of Representation and Interpretation," as his work of the same name suggests. This sense of "other" is critical to ciphertext, and lies behind the claims of secrecy (which, as I mention, is only one of many positivities). In fact, as I discuss with respect to the parallels between Gaviria's art and its military origins, secrecy is historically and contextually particular, but related to otherness, which is created by ciphertext. In the end, Gaviria's art helps us understand how code vacillates between plaintext and ciphertext, as forms of representation and interpretation, to reveal and enclose hidden orders.

Order is an important quality of ciphertext, which is, at least as it pertains to ciphertext, perspectival. Consider the fact that ciphertext is only hidden, secret, or mysterious in certain contexts and from certain perspectives. When, for example, cryptography is used for cybersecurity today, the resulting of ciphertext resembles noise, or pure chaos for stymying human eavesdroppers. Phenomenologically, such ciphertext has the appearance of being "other." In this chapter, the focus is on the latter, on understanding how order can potentially interact with the "other." The "other" of ciphertext, however, is not the radical, absolute, or pure Other of some common deconstructionist theories, nor those of the mystic or religious. Rather, ciphertext is designed by human creators to be very good at "hiding" a *meaningful order* (the plaintext) within a more *complex order* (the ciphertext). Therefore, the "other" of ciphertext is, ultimately, an illusion.

The transformation from plaintext to ciphertext *appears* to work in ways that are opposite to nature. Order that results from creation in the divine sense, as well as the technical or artistic senses, is usually understood to be a process that

goes from the formless (or unordered) to the ordered. For example, in his *Theogony,* Hesiod wrote about the undifferentiated mass of the universe before order was applied, to cleave heaven and earth; or consider Anaximander's *apeiron,* which was believed to be an originary, formless continuity. In most western, Christian thought, God creates something out of nothing, ex nihilo. When God creates ex nihilo, however, He orders, and also makes knowable the word (*logos* is as much about creation and language as it is order). Humankind can only know that which is ordered, which is why when we think about the creation of technical or artistic artifacts we usually think about the formless becoming more knowable (e.g., the sculptor shapes the clay into a Roman bust). The opposite process is destruction—to render something unordered and therefore unknowable.

Superficially, cryptography appears to operate in these terms, distinct from how we think technical and artistic production works—to encrypt is to create something unknowable from the knowable. With encryption, it is as though the knowable has become unknown—*as if* destroyed. From the limited perspective of the person looking at ciphertext, the artifact does appear to have been destroyed. But, from the "perspective" of a philosopher's omniscient god, indeed, nothing has been rendered unknowable, and nothing has been disordered. Gods, *and machines*, are not so limited in perspective, and thus do not experience *our* ciphertext as "other." Of the unknowable, in fact, we can imagine that an omniscient God does not see the mystery and otherness of ciphertext—He sees the world as only plaintext.

This human illusion works by creating a "higher order" or "more complex" sense of order in ciphertext, which renders plaintext unknown. Creating this illusion of otherness through order is an illusion of radical transmission, from humans to gods. If such an activity were truly "real" it would require a mediator capable of bridging two radically Other worlds. I called these illusory mediators "angels" in chapter eight. Elaborating on the previous description, we will see in this chapter that such angels are a *necessary illusion* for the encryption process. That is, from the limited perspective of humankind, the gulf between plaintext and highly ordered ciphertext is too great to be crossed without aid. In this chapter the concern is with the illusion itself—with the ways that technological means lets humankind create forms of order that seem to reach beyond our limited capabilities and perspective.

10.1 CRYPTOGRAPHIC ORDER

"The universe believes in encryption." [1]

Ciphertext requires the precise application of order; any variances from the prescribed method are potential weaknesses and subject to cryptanalysis. The marvelous thing about the rise of cryptography over the last few decades is that computation has become so cheap, and analytical methods have become so powerful, that the only significant issues remaining for the production of strong (even unbreakable) cryptography are human errors, primarily related to software development. Bugs in software development are, invariably, the wedge that cryptanalysis applies today. On the other hand, we also have good measures of the strength of cryptographic primitives.

Cryptographic strength is a measure of the perceived disorder of ciphertext, and the perceived disorder of ciphertext is an expression of the degree of entropy, which, in the Shannon sense, is a measure of the unpredictability of the message. These measures exempt innovations in fundamental aspects of mathematics, such as the discovery of a new way to perform fast prime factorization. Typically, this order is modeled as a Markov chain, as Shannon described in his "A Mathematical Theory of Communication."[2] Measurement of Markov chain elements determine the statistical likelihood of dependent prior elements in a stochastic sequence. Therefore, with this technique, the relationship between each element of ciphertext is given statistical measure, which determines the degree of variance from pure randomness, or chaos. When ciphertext has complete entropy, or *chaos* (maximum information), it has no statistical measure, and so, a completely entropic ciphertext could in theory contain any plaintext (or alternatively, no plaintext).[3]

The engineering techniques developed for measuring order in ciphertext are very useful and important, but they are only a small part of the study of order (and correspondingly, only a small part of the study of ciphertext). Order, itself, has become a vast and important topic of study. Over the last century order has become a subject of the disciplinary study of mathematics (a historical development that Shannon was quick to draw on). This shift towards the

[1] Assange et al., *Cypherpunks*, 4.
[2] Shannon and Weaver, "A Mathematical Theory of Communication."
[3] This presupposes limitations on channel capacity (Shannon coding), or semantic equivalences. It may be philosophically sensible to say that this *iota* contains or represents the infinity of the universes, but such questions are of no interest to engineers like Shannon.

mathematical study of order parallels the instrumentalization also seen in the study of cryptography, and no doubt the two are historically related (an issue only alluded to here, but deserving of further investigation).

This history of the study of order begins to really gather steam following Leibniz in the seventeenth and eighteenth centuries, who subjected the systematic analysis of order to combinatoric analyses (combinatorics is the study of finite discrete things, or countable objects, and their relationships and arrangements).[4] Therefore, through the eighteenth and nineteenth centuries, combinatorics then became an important tool for the mathematical study of finite things (many of these studies started earlier, in a incubatory state, with an interest in "magic squares," games of chance, acrostics, and cryptography).[5] By the middle of the twentieth century, the combinatorial study of cryptography became associated with informatics, also in large part due to Shannon's use of Markov chains for the analysis of secure systems. Similarly, at the same time that combinatorics became an important topic for mathematical investigation, the investigation of physical manifestations of order became an important topic for scientists.

Although there is a great deal of potential pre-history, the rational development of combinatorics in the West has been attributed to Leibniz (the Arabs, as described in chapter nine, also had well developed combinatorial techniques as part of their cryptanalysis and translation efforts).[6] In this regard, Leibniz was influenced by the Lullian tradition as it swept through modern science, as well as the universal language planners' activities.[7] In his *Dissertatio de art combinatoria* Leibniz described important combinatorial principles, referencing Lull explicitly. There is also the possibility that Leibniz, as an ardent

[4] See chapter five for an illustration of how Leibniz used notation to investigate combinatorial relationships.

[5] Biggs mentions "magic squares" which are very similar to acrostics and the tables used for enciphering and cryptanalysis. See Strasser, "Ninth-Century Figural Poetry and Medieval Easter Tables—Possible Inspirations for the Square Tables of Trithemius and Vigenère?"; Leary, "Cryptology in the 15th and 16th Century" For some historical examples. Biggs also mentions games of chance, including techniques developed by Cardano (an important universal language planner), Galileo, and Pascal. See Biggs, "The Roots of Combinatorics."

[6] There are in fact a number of mathematical precursors, including Mersenne, Schwenter, and Christoph Clavius, see Knobloch, "The Mathematical Studies of G.W. Leibniz on Combinatorics" for an extensive discussion of the history of combinatorics.

[7] See chapter four for a description of the notational discourse network within the universal language planning movement. Lull is explicitly mentioned by Leibniz in his *Dissertatio*, but there is reason to believe that Lull's style of computation differed in important ways from Leibniz (most notably, Lull's mathematical naivety); see Uckelman, "Computing with Concepts, Computing with Numbers."

Sinophile, might have been inspired in combinatorial mathematics by the *I Ching*, primarily through his correspondences with Bouvet.[8]

In his *Dissertatio*, Leibniz described a mathematical technique for the analysis of order. Leibniz characterized order mereologically, as the differences between parts and wholes, which can be calculated with regard to the variety of ways that they can be arranged and put together. There are, according to Leibniz, two ways to understand the "variation" of parts and wholes: complexion and permutation, which are both processes of change of relation.[9] "Complexion" is Leibniz's term for what is now called "combination" (Leibniz reserves the term "combination" for his notation of different kinds of order). Within complexions there are different ways of arranging the parts, which Leibniz calls "*situs.*"[10] So-called "absolute *situs*" are relations between the part and the whole, which is the number of places or distance between the whole and the parts; "relative *situs*" are relations between parts and parts, which is the distance between the parts. For Leibniz, the relations of part and whole, absolute *situs*, are specifically the properties of "order."[11]

Leibniz offers some concrete examples of how "by reason of order the following *situses* are different ABCD, BCDA, CDAB, BABC [*sic*]."[12] Specifically, the order of the complex ABCD can be analysed in terms of bigrams (what Leibniz described as "com2nation," using his notation adopted from Marin Mersenne): AB, AC, AD, BC, BD, CD; or in terms of trigrams ("con3nation"): ABC, ABD, ACD, BCD (Leibniz considers bigrams and trigrams without reference to place, so, AB = BA). From this, the entirety of complexions can be computed, e.g., 15 is the computed total from all 4 parts: (4 units, 6 com2nations, 4 con3nations, 1 con4nation; 4+6+4+1=15).[13] Leibniz offers a table of these computations (figure 10.1), which is schematically and analytically very similar to how cryptanalysis permutations are calculated.[14]

---

[8] The I Ching combines two symbols (the Yin and Yang) to form hexagrams, which were at times used for systematic ordering. The exact use of this ordering, from the earliest times, however, has been called into question. Leibniz seems to have been mislead on this point, and on his authority a long history of this mistaken view that the *I Ching* birthed binary arithmetic has persisted; see Biggs, "The Roots of Combinatorics.". See also Berkowitz and Cook, "Leibniz-Bouvet Correspondence."

[9] Leibniz, "Dissertation on the Art of Combinations," 77.

[10] Ibid.

[11] Ibid., 78.

[12] Ibid.

[13] Ibid.

[14] See chapter nine for detail on medieval Arabic cryptanalysis and the use of permutation tables.

TABLE ℵ

0	1	1	1	1	1	1	1	1	1	1	1	1	1
1	0	1	2	3	4	5	6	7n	8u	9m	10b	11e	12r
2	0	0	1	3	6	10	15	21	28	36	45	55	66
3	0	0	0	1	4	10	20	35	56	84	120	165	220
4	0	0	0	0	1	5	15	35	70	126	210	330	495
5	0	0	0	0	0	1	6	21	56	126	252	462	792
6	0	0	0	0	0	0	1	7	28	84	210	462	924
7	0	0	0	0	0	0	0	1	8	36	120	330	792
8	0	0	0	0	0	0	0	0	1	9	45	165	495
9	0	0	0	0	0	0	0	0	0	1	10	55	220
10	0	0	0	0	0	0	0	0	0	0	1	11	66
11	0	0	0	0	0	0	0	0	0	0	0	1	12
12	0	0	0	0	0	0	0	0	0	0	0	0	1
*	0	1.	3.	7.	15.	31.	63.	127.	255.	511.	1023.	2047.	4095.
†	1.	2.	4.	8.	16.	32.	64.	128.	256.	512.	1024.	2048.	4096.

Exponents — Complexions

Figure 10.1: Table of Complexions and Exponents.[15]

In addition to providing a technique for calculating the order of alphabetic parts (no doubt useful for cryptanalysis), Leibniz described the ways that this analysis of order can also be used for a variety of real-world practical applications. Science, for example, provides multiple opportunities for combinatorial analysis, including the division of natural creatures into species and genus, and the division of attributes. Leibniz also saw his technique as useful for determining the "compounded medicaments and pharmaceuticals… made by mixing various ingredients."[16] Leibniz's technique also enabled the calculation of the number of notes that can be played on an organ, and the division of a variety of theological notions,[17] much like Lull's prior attempts. In fact, Leibniz even developed a wheel, styled like Lull's, for combinatorial analysis of the traditional natural qualities (earth, air, fire, water) (figure 10.2).

[15] Leibniz, "Dissertation on the Art of Combinations," 79. The table is used to "discover the complexions [combinations] for a given number and exponent." The top x-axis line is an additive use of 0 and 1, anticipating Leibniz's interest in a binary number system. The left y-axis line are the exponents. The bottom two x-axis lines are 2^n and 2^n-1 (where n=the exponent under consideration). The calculated values are the "total complexions [combinations]." Leibniz gives the following instructions for use: "Add the complexions of the number preceding the given number, by the given exponent and by the exponent preceding it; the sum will be the desired complexions. For example, let the given number be 4 and the exponent 3; add the 3 com2nations [exponent 2] and the 1 con3nation [exponent 3] of the preceding number 3; (3+1=4). The sum 4 will be the answer." In his example, the "given number… 4" is the fifth 1 from the left on the x-axis, and the exponent is the third down from the top on the y-axis.

[16] Ibid., 81.

[17] Ibid.

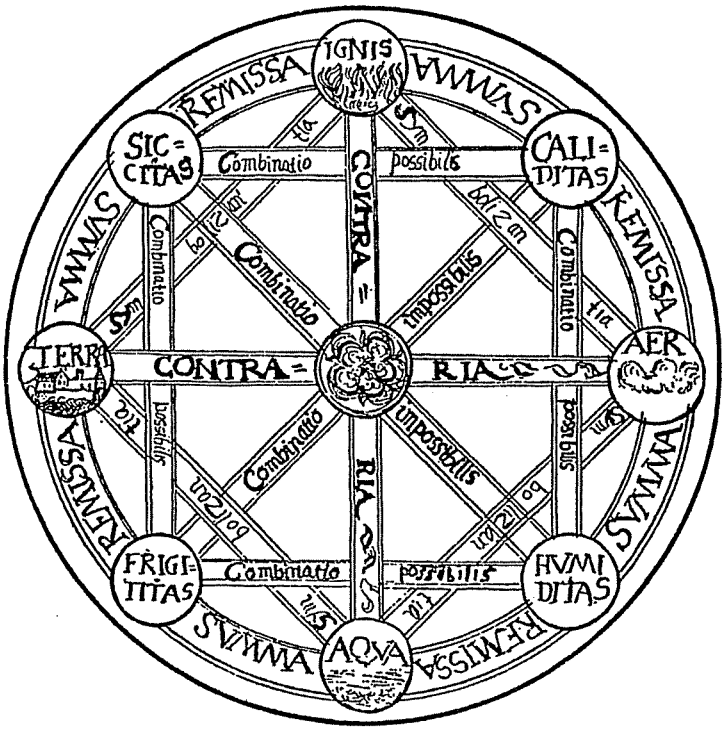


Figure 10.2: Leibniz's wheel of combinations.[18]

Using the knowledge gained during these early investigations into combinatorics,[19] Leibniz later designed two machines to actualize these theoretical notions. The more famous of his two machines, the "stepped reckoner," has been the subject of many historical treatments, and lauded as an example of early computing.[20] This calculating device was impressive for both its technological sophistication and analytical foresight. More sophisticated than Blaise Pascal's addition and subtraction device, Leibniz's device could multiply and divide as well, which enabled a large number of analytical techniques. The core technology of his calculating machine was a stepped drum mechanism from which the device gets its name (in German, "*Staffelwalze*"). The calculating machine used a number of stepped drums, each affixed with what we now call a "Leibniz wheel."

In a simplified form of the calculating machine (using only a single stepped drum in its design), Leibniz also planned, but seemingly never built, an

[18] Ibid., 83.
[19] Leibniz later shied away from this work, realizing its structural deficiencies and overreliance on Lullian themes, but he maintained that it was correct in its basic approach.
[20] See, for example, Davis, *The Universal Computer the Road from Leibniz to Turing*.

enciphering and deciphering machine. The inspiration for his cipher machine came from his success with the calculating machine: "this arithmetical machine led me to think of another beautiful machine that would serve to encipher and decipher letters, and do this with great swiftness and in a manner indecipherable by others." Unfortunately, perhaps due to the traditionally secret nature of cryptological activities, Leibniz never fully described the machine, and little is known about it. Digging through Leibniz's scant mentions of it in his personal papers, and using the calculating machine as a guide, Leibniz historian Nicholas Rescher has worked out a conjectural description of the cipher machine.[21]

Leibniz's cipher machine was to be used for encrypting and decrypting in much the same way as Alberti's cipher wheel, which rotated through the alphabet to associate a new index letter for each encryption step, producing polyalphabetic encryption.[22] Leibniz's cipher machine, however, automated Alberti's manual process of selecting new alphabets, and added a number of levels of cryptographic complexity. To encrypt (or in reverse, decrypt), the stepped drum would rotate a set amount (60 degrees in Rescher's conjectural description) for each *N* keypresses, where *N* is set by a special control mechanism. Therefore, a new alphabet would be introduced at this set interval of keypresses. The index letter permutations would be set by moving wooden slats (establishing the correspondences between the "key" positions and the plaintext), not unlike Kircher's musical *Arca Musarithmica* or his more general, and mathematical, *Organum Mathematicum*.[23] As the operator inputs a message (using a keyboard adopted from a "clavichord or other instrument"),[24] the machine simultaneously encrypts and decrypts, showing both the encryption and decryption results in their designated boxes. To encrypt a message, the operator arranges the wooden slats and the stepped drum control, noting (and keeping secret) the selected configuration. The operator then enters the plaintext with the keyboard, and writes down the corresponding ciphertext. To decrypt a message, the operator reverses the process: arranging the wooden slats and stepped drum controller to match the original (encryption) setting, entering the ciphertext on the keyboard, and reading the plaintext results from the appropriate (decryption) box.

[21] See Rescher, "Leibniz's Machina Deciphratoria."
[22] See chapter three for a discussion of Alberti's cipher wheel.
[23] See chapter four for a description of Kircher's inventions.
[24] Rescher, "Leibniz's Machina Deciphratoria," 104.

10.1.1 The study of order

Following Leibniz, combinatorics and the study of order developed further. Many of the early histories are also reflected in the later developments, too. Consider Nobel Laureate Wilhelm Ostwald, who, in the nineteenth century, applied the processes of combinatorics analysis to chemistry, which he used to calculate the number of isometric substances in advance of experimental confirmation (with clear allusions to Leibniz's use of combinatorics for "compounded medicaments and pharmaceuticals"). In fact, part of Ostwald's legacy, the subdiscipline of combinatorial chemistry is still highly active today. Similarly, like many of the universal language planners before him, who used combinatorial techniques to organize knowledge,[25] Ostwald also attempted to construct a universal encyclopedia, as well as a rational organization of aesthetic principles. Ostwald had even broader ambitions, setting his sights to establish a "science of order" that he called "Mathetics."[26]

It has also become fashionable to invoke the study of order, but more particularly, chaos, in philosophical and literary traditions. Hayles, for her part, identifies many ways that art, literature, and science co-determine each other in the study of chaos and order. Many poststructuralists and deconstructionists, especially those looking for instabilities to act as a pry bar for critique, have also turned to the study of chaos. Hayles notes that "where scientists see chaos as the source of order, poststructuralists appropriate it to subvert order."[27] Sometimes these attempts are successful, sometimes they are not.

The study of order, without strong reference to chaos, has also been a topic of social and political critique, and has, in my opinion, proven more successful. Unlike some of the poststructuralist authors, these studies tend to avoid the strong equivocations between mathematical, scientific, and literary studies of order. For example, Eric Voegelin's five volume *Order and History* finds the basis of order in the "ground of being," which, for Voegelin, is the divine. Voegelin sought to understand the "order of man, society, and history to the extent to which it has become accessible to science." Similarly, Michel Foucault studied epochs of order to understand how things become objects, and to understand how humankind itself became a subject.

In *Order of Things*, Foucault described order as that "which is given in things as their inner law."[28] According to Foucault, this order lays hidden until its

[25] See chapter four for a discussion of universal language planners.
[26] Hapke, "Wilhelm Ostwald's Combinatorics as a Link between In-Formation and Form," 288.
[27] Hayles, *Chaos Bound*, 176.
[28] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, xxi.

moment of expression. Order is "the grid"—a "middle ground" between domestic and scientific realities—that is created by "a glance, and examination, a language."[29] At the middle ground a culture can deviate from empirical orders, such that it can free itself to discover that its current order is not "the only or possible… or the best…."[30] This middle ground is the "most fundamental of all," where reality is "anterior to words, perceptions, and gestures" in which "there is the pure experience of order and of its modes of being."[31] The middle ground is precisely where we find Foucault's famous historical *a priori* and his study of order, which establishes what "ideas could appear, sciences be established, experience be reflected in philosophies, rationalities be formed."[32] These ideas, sciences, experiences, and rationalities are ordered on a grid or tabula, which shifts and changes—stabilizes and destabilizes—in response to social and technological changes (apparatuses, or *dispositif*)[33] within distinct eras (*epistemes*).

Foucault's investigation positions order as a foundational aspect of social change—responsible for, and responsive to, changes in art, science, politics, and even morality. Foucault's critical project relies on his concept of a priori history, which is not "determined by what is called the mentality of the 'framework of thought' of any given period."[34] Rather, the *a priori* of "any given period… delimits… the totality of experience…, [and] defines the mode of being of the objects that appear in that field."[35] In other words, order is, for Foucault, both a stabilizing force and an agent of change, depending on who, and what, interacts with the numerous levers.

Foucault's work shows how the normative valences of the grid of order and the associated ordering apparatuses are subject to critique and change. And as much as power can (and does) structure and ossify, the grid structure is also mutable. One result of the normative nature of order is that it implies that there is no single perspective from which to approach order in the world. Foucault's study of order also demonstrates the apparent limitations of critical perspectives on actual forms of order, which are in fact not fully determined by the individual. Order can be best perceived at cultural (or "schematic") scales, or in rare cases, at the interstices and cracks that form in the representational

[29] Ibid.
[30] Ibid., xxii.
[31] Ibid., xxiii.
[32] Ibid.
[33] Agamben, *"What Is an Apparatus?*
[34] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, 172.
[35] Ibid.

undergirding. Indeed, the hardest orders to change are the broad social, scientific, and artistic ones, because these are precisely the kinds of actions and objects enabled and constrained by order.

10.1.2 Perspectival ordering

> *The notion of order… extends beyond the confines of a particular theory; permeates the whole infrastructure of concepts, ideas, and values; and enters the very framework in which human thought it understood and action is carried out. To understand the full meaning of creativity and what impedes it, it is necessary to go into the whole nature and significance of order.*[36]
>
> *Order [is] the degree and kind of lawfulness governing the relations among the parts of an entity.*[37]

Order resides in systems that are complex, have distinct parts, may be either quantitative or qualitative (binary), have necessary relations among parts, and are lawful (principles that governs the relations among parts), according to Lorand's general theory of order. Lorand introduces two senses of the word "order," both of which are important to ciphertext: 1) the *ordering principle*, which is a law, rule, pattern, or form by which elements may be arranged, 2) the *condition of a given set*, that is, its conformity to the ordering principle.[38]

Lorand points out that order depends on the ability to perceive similarities and differences.[39] This, she notes, was already well understood by Leibniz. For example, atoms—Leibnizian monads—have no inner order because they are simple.[40] Similarly, totally homogenous systems cannot have order. Complexity, however, is comprised of simple entities, and complexity is a necessary but not sufficient condition for order.[41] Complexity is not a sufficient condition for order because complex objects may be disordered. Ciphertext is complex in that the order is comprised of atomic elements (plaintext notation). At some levels of complexity, the ordering principle becomes obscure and unknown, and the complexity of order surpasses human ability to comprehend and understand—thus, becoming the "other" of ciphertext.

Simple and complex are matters of perspective and context—that is, objects may appear less complex for psychological or pragmatic reasons. Individuals

[36] Bohn and Peat, quoted in Lorand, *Aesthetic Order*, 7.
[37] Arnheim, quoted in Ibid., 9.
[38] Ibid.
[39] Ibid., 10.
[40] Leibniz, "The Monadology."
[41] Lorand, *Aesthetic Order*, 10.

may perceive different levels of complexity when viewing the same object on account of training, interest, or other psychological factors. This implies that differences of perceptions of complexity are due to the application and recognition of different ordering principles (which is why, for example, a botanist walking through the woods sees a rich world of different objects and relations, while a casual hiker sees only so many unvarying trees, rocks, and bushes). Order also matters when grouping things together, because of the differences of perspective and context. Lorand defines "class" as "all sets that are ordered by the same ordering principle."[42] The idea of a "maximum" level of complexity is likewise flexible, depending on the individual and the context. Most ciphertext exceeds any realistic expectations of human perception of complexity, and thus any ability to make determinations of the degree of complexity is thwarted. When a maximum level of complexity is exceeded, the ordering principle becomes perceptually obscure, and the entity—here, ciphertext—effectively becomes simple (and not ordered), as though an unvaried and continuous mass.

Even though order is perspectival and context sensitive, it is still possible to have qualitative/binary orders, or even quantitative ones. In fact, quantitative order is more typically found in cultural and empirical contexts, which are assessed by the degree of adherence to the ordering principle. For example, a country ordered by a democratic principle may be more or less ordered (quantitatively), according to the degree to which the state adheres to the principle of democratic ordering. A game of chess may also be assessed quantitatively—the degree to which a particular game is played according to some optimal set of moves. If, however, the rules of chess are not adhered to during play, the ordering principle is dismissed and the game ceases to be chess at all; the very concept of the game of chess is evacuated. In the latter case, rule-following in chess is a qualitative or binary ordering principle ("is chess? is not chess?".

Clearly, encryption—and decryption—are binary orders, like chess. Non-compliance to rule following does not result in "less cryptography," it simply results in a scrambled mess. The encryption process either orders atomic items (notations) in strict accordance to an ordering principle, or it fails to be encryption at all. Cryptanalysis, on the other hand, is a process of quantitative ordering. When some "non-decryption" technique is used to guess a plaintext from a ciphertext, the result is necessarily some *degree* of compliance to a (hidden) order. That is, cryptanalysis is measured by its degree of adherence to

[42] Ibid., 11.

some unknown ordering (the encryption/decryption process). For this reason, statistical measures are often used to aid the cryptanalyst,[43] providing a tangible measure of the degree of confidence towards a particular result.

Order always entails necessity, but necessity does not always entail order. An ordering principle requires, postulates, or defines certain relations, rather than constrains or determines them (e.g., the expression "all numbers less than 5" is not an ordering principle, but "every odd number" is).[44] Order and relation are two interconnected notions, in that relation does not imply necessity, but order does. Only when a relation is induced by an ordering principle does it express some kind of necessity. For example, as described in chapter nine, in Leibniz's *Dissertatio* the relations between AB, AC, AD, BC, BD, CD and ABCD are necessary because the bigrams are an exhaustive description of the permutations of the class. Necessity, however, like order itself, is also perspectival, in the sense that the ordering principle may not be immediately obvious, or understood.

Ciphertext is a perspectival form of order, and especially so. Such a view may suggests a "subjective" ontology for ciphertext. But, the nature of "subjective" and "objective" can, Lorand notes, mislead if used in their extreme senses. Whether something can exist in a purely subjective, or, on the other hand, a God-like objective sense, is a problematic idea, given post-Kantian critical philosophy.[45] Order that is entirely independent of an observer's contribution or qualification would be unknown, according to Kant. For the notions of aesthetic order that concern Lorand, Kant's limitations are extremely important provisos for recognition of the perspectival nature of order. Ciphertext, however, complicates Kant's limitations, since the very nature of ciphertext is to strive to remain unknown and other. It is a curious fact about ciphertext in society that there exists the possibility that some hitherto "objective" order may be one day discovered in any entity, of any kind.

Technical applications of ciphertext, by design, work very hard to remain unknown, incomprehensible, and "other"—admitting very little comprehension of their ordering principles. To better understand the application of these ordering principles, and to see how ciphertext can be revealed in social, political, and philosophical contexts, I describe a case study of artistic practices that interrogate these relationships.

[43] See chapter nine for a description of the systematic processes of cryptanalysis.
[44] Lorand, *Aesthetic Order*, 18.
[45] Kant, *Critique of Pure Reason*, 129 ff.

10.2 Andrés Ramírez Gaviria: "Between Forms of Representation and Interpretation"

Andrés Ramírez Gaviria's art is important for understanding cryptography because it reveals and critiques the otherness of code, through order and perceived disorder, in an aesthetic form. To do so, Gaviria uses a range of materials, including microcontrollers, aerospace and hi-tech materials, strobes, sound performances, chopped and cut video, printed text, and images.[46] As with other "new media" artists, Gaviria's work simultaneously responds to, critiques, and embraces research and development in cybernetics and informatics through the mid-twentieth century, in ways that parallel developments in cryptography. Gaviria's work uses a variety of processes of transcription and transmission to expose hidden, and yet, in today's society, dominant, representational pathways. Through these methods, Gaviria seeks to understand code and order at the interstices of language and thought, which, he argues, lie "between forms of representation and interpretation," as his work of the same name suggests.

Since Edward Snowden's global surveillance disclosures in 2013, Gaviria's work has taken on a political valence. On a historical level, Gaviria's work shines a light on the ways that this global control apparatus stems from the last century's mathematical theories of secrecy and information (as exemplified by Claude Shannon's work).[47] Gaviria's work also seems to suggest that this global control apparatus is found in everyday communication, and is today impossible to comprehend.

Through an analysis of Gaviria's art, I draw parallels to the ways that military and security research intersects with developments on language and ordering technologies, and therefore, ask what this means for us today, the consumers of this discourse network. It is an obvious truth that our world is characterized by digital technologies, as it was in the 1950s too, when, for example, vast mainframes calculated airline reservations (SABRE) and automatically processed checks (ERMA). However, something has changed in the last few decades. From these digital technologies there have new ways of understanding people and things, which now operate in black boxes, filled with secret codes. It is a critical task of those who study this coded world—scholars, artists, politicians, and all—that new linkages may be drawn and assessed.

---

[46] An earlier version of this section appeared in DuPont, "Otherness and Order."
[47] Shannon, "A Mathematical Theory of Cryptography"; Shannon and Weaver, "A Mathematical Theory of Communication." See also chapter one.

One critical moment in this transition to new ways of ordering people and things arose at Lincoln Laboratory at MIT, which was conducting research on interactive computing for military command and control throughout the 1960s and 70s. Gaviria's work interrogates the origins of modern computer aided design (CAD), through two examples of Ivan Sutherland's Sketchpad software. The design and development of this early CAD system required answering deep questions about the ways that mimetic forms of representation (sketching, speaking) were, or were not, still suitable foundations for tools driven by code, an issue I discussed previously in chapter three. Gaviria's work probes these questions by actualizing CAD drawings generated from the machines developed at Lincoln Laboratory: with "Untitled (Monument)" Gaviria fabricates a CAD drawing out of wood—teetering, imposing, and at large scale. These works blur those supposedly natural categories of sketching and speaking, and when Gaviria brings them to life we are forced to reconcile their underlying code and the realized form.

In fact, Gaviria probes language, our "fundamental" conduit, over and again until it blurs into code. Gaviria's ".-/" offers an account of information and communication technologies, reworking Kandinsky's original by applying its own inner logics to a new production. The result is that, in this artwork, this printed book became, in fact, optimized for transmission. As a prospective reader, Gaviria's reworked "book" is stupefying, alien, and other. Manifestly, one does not "read" Gaviria's ".-/"— it can only be deciphered.

Gaviria's most prescient and political work, "Beyond Black," offers further commentary on our ubiquitous codes today. These shiny black panels are reminiscent of the National Security Agency (NSA) BLACKER project. What this work demonstrates is that surveillance and cybersecurity technologies are built at, by, and for, non-human scales. At these scales, "real" or "natural" perspectives of hidden order are illusory.

10.2.1 Art at the intersection of code and mimesis

In "Untitled (Monument)" (2013; figure 10.3) Gaviria interrogates a critical juncture of the history of cybernetics with his wooden fabrication of one of the first ever technical models designed on a computer. The large wooden object teeters uncomfortably, literally reminiscent of a design with no intention to ever be built. The sharp lines and uncomfortable shape contrast with the odd choice of product, a wood so deeply grained that its seams are still visible. These seams, too, are surely a product of its material construction, smoothed over by Gaviria but absent in the original CAD drawing.

Figure 10.3: "Untitled (Monument)."

This work refers to an important video of the complex 3D shape displayed with Sketchpad, Ivan Sutherland's PhD dissertation software built at Group 51 in Lincoln Laboratory, an applied research lab at MIT. In this video, filmed some time after 1964, Sutherland is absent, by then working at the NSA designing computer displays, presumably to aid cryptanalysis efforts. In Sutherland's place are Timothy Johnson and Lawrence Roberts, then researchers at Lincoln Laboratory, responsible for helping build Sketchpad (Roberts, in particular, went on to an illustrious career at ARPA Information Processing Techniques Office, creating essential aspects of today's Internet). In the video, the pair show the operations of Sketchpad running on the experimental TX-2 computer (the TX-2 was a successor to TX-0, an early interactive computer) . Johnson shows many of the 2D operations developed by

Sutherland (and subsequently refined by Johnson himself for his 1963 Master's thesis),[48] followed by Roberts showing the 3D operations that he developed.[49]

In the video, Roberts shows a strange shape being rotated in perspective view—perhaps the design for a "piece of wood," Roberts suggests. In "Untitled (Monument)," Gaviria fabricates Roberts' object in large scale—as a piece of wood.

The "piece of wood" Roberts shows in the Lincoln Laboratory video was originally designed for Roberts' PhD dissertation.[50] In his dissertation, Roberts offers two images of the "piece of wood," originally labelled "Compound Object" and "Rotated View of Object" (see figure 10.4). It is unknown if "Compound Object" started life as a physical object—a prototypical "Untitled (Monument)." It is possible, since many of Roberts' examples are in fact photographs of physical objects that were subsequently digitized in Sketchpad (such automatic digitization of objects was the main focus of Roberts' dissertation).

[48] Johnson, "Sketchpad III, Three Dimensional Graphical Communication with a Digital Computer."

[49] Johnson was working out of MIT's Computer-Aided Design group, a separate entity, so while Roberts and Johnson shared the TX-2 computer and Sutherland's Sketchpad code base, they worked at some distance.

[50] Roberts, "Machine Perception of Three-Dimensional Solids."

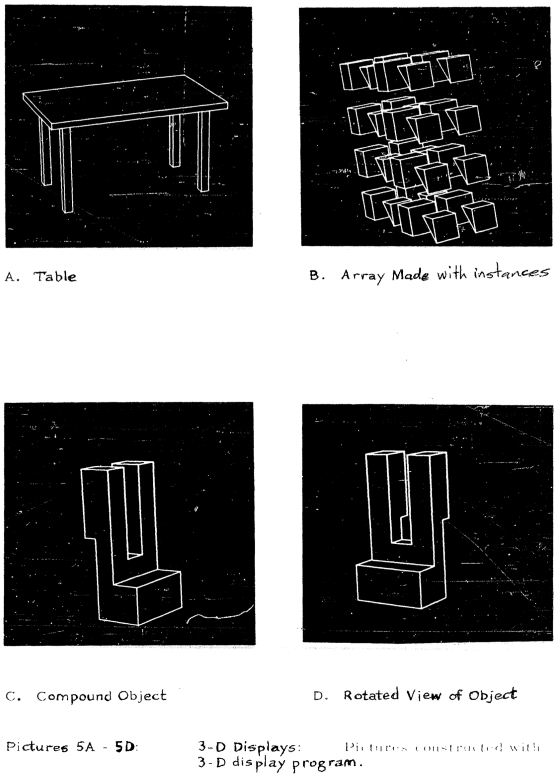


Figure 10.4: "Compound Object" and "Rotated View of Object."[51]

This graphics research was cutting edge, since even the ability to issue a command and receive an immediate response from a computer was basically unprecedented at the time. Thus, the idea of virtually manipulating 3D drawings such as the "Compound Object" must have seemed otherworldly. But despite the compelling demos, the Computer–Aided Design idea was really just an example of interactive computer control, which was the original goal of the TX-2 computer and the broader vision for the Sketchpad research programme.

The interactive computer work performed at Lincoln Laboratory was funded for the purpose of improving military command and control processes. Interactive computers and software were designed to be able to compute and analyze increasingly large and complicated military data stores. Advanced, high speed input and output was a necessary practical development for interaction with these data stores. This research was seen as necessary for air defence technologies, a pertinent concern at the time, as cold war nuclear threats were escalating (since 1949 the Soviets had nuclear-capable long-range aircraft that could evade the existing Ground Control of Intercept radar system).[52]

[51] Ibid., 70.
[52] Grometstein, *MIT Lincoln Laboratory: Technology in Support of National Security*, 1.

Prior to Sketchpad, Lincoln Laboratory made its name in research for radar systems. Project Whirlwind, initially built at Lincoln Laboratory for aircraft simulation, became a real-time computer used for processing and coordinating radar signals from the Semi-Automatic Ground Environment (SAGE) system of radars. Building on the Whirlwind research, Lincoln Laboratory developed fast memory, interactive displays, and advanced software programming techniques for the TX-0 and TX-2 computers (these were effectively transistorized successors to Whirlwind I and II, and IBM's AN/FSQ-7 Combat Direction Central computer used for SAGE). On account of the success of the TX-2 computer and Sketchpad, IPTO would continue to fund projects investigating human-computer interaction, leading to designs to link machines for resource sharing—what would eventually become the ARPANET and the modern Internet.[53] Today's modern command and control infrastructure is in every way involved in these developments at Lincoln Laboratory.

While some of the general 3D functions for Sketchpad were developed by Johnson, it was Roberts who made 3D display possible. Roberts developed the mathematics and algorithms for hidden line removal—an important contribution to the history of computing, which provided Sketchpad the ability to display solid 3D objects (rather than just wireframes) while occluding certain parts that are out of the field of vision. Neither Gaviria's physical "Untitled (Monument)" or Roberts' CAD "Compound Object" drawing is visible in its entirety from any one perspective. Therefore, the physical object and the computer renderings require *interaction* to gain a fuller perspective. 3D CAD design would be impossible, as we know it, without interactive computing. Indeed, perspective, or lack thereof, is a constant theme of Gaviria's coded art.

In the Sketchpad video, Steven Coons[54] describes this mode of interaction as "talking" to the computer. Similarly, Sutherland describes Sketchpad's mode of interaction as human "conferring" with the computer. Drawing, Sutherland thought, was a step better than "[reducing] all communication to written statements that can be typed."[55] However, Sutherland soon realized that while this interactive mode of interaction was valuable, because it enabled the designer to roughly "sketch" an idea like drawing, it was the subsequent use of notational constraints that allowed the operator to hone the sketch into a technical document. The technical document, unlike the rough sketch, could

[53] Norberg, "Changing Computing," 43.
[54] Co-director of MIT's Computer Aided Design group and a member of Sutherland's dissertation committee.
[55] Sutherland, "Sketchpad: A Man-Machine Graphical Communication System," 8.

then be modularly edited, reordered and reconfigured, and duplicated with ease. It is precisely these notational affordances that make the use of Sketchpad quite different from normal kinds of drawing.

According to the TX-2's principle designer, Wesley Clark, the TX-2 was originally conceived to make possible a Sketchpad-like application.[56] The TX-2 had high-capacity, fast memory, which made real-time storage and retrieval of the screen "dot" locations a practical possibility. The dots were generated on a 7" oscilloscope, and controlled using a light pen—technologies perfected at Lincoln Laboratory for use with the Whirlwind computer's display for radar tracking. Interactive sketching was accomplished with the light pen, which moved the cursor across the screen, and with the press of a button dropped virtual pins connected with a rubber band effect to stretch out lines or simple curves. After a line had been created its properties and position could be numerically edited and adjusted using a number of design capacities and constraints that Sutherland built into Sketchpad.

When Sutherland was designing Sketchpad he had to come up with new kinds of human-computer interaction, and new kinds of representation. At first, he saw himself as emulating a drawing process, but "it has turned out that the properties of a computer drawing are entirely different from a paper drawing."[57] Sutherland soon realized that he would need to rethink what representation for CAD means—drawing on a computer, as Gaviria strikingly points out, is "between forms of representation and interpretation" and thus needs new methods.

Sutherland's efforts at designing new kinds of representation suitable for computer aided design can be contrasted with the field's proto-origins, as found in Leon Battista Alberti's *Descriptio vrbis Romæ* (see chapter three). Recall that the *Descriptio* was a coded (notational) method of design that worked to remove the erring, sloppy, and imprecise craft element from architecture; in Alberti's hands, architecture became a science. The *Descriptio* was a mechanical device, basically a round plate or horizon with a ruler affixed to its center, that converted coordinates to points, which could then be connected using a variety of predetermined line types (straight or curved). Armed with survey data of the city of Rome and the *Descriptio* mechanism, a perfect copy of the plan of the

[56] By 1966 the TX-2 would also be used for early interactive computer networks, see Hemmendinger, "Two Early Interactive Computer Network Experiments."; the TX-2 would also find some application for early speech recognition applications, image processing, and experimental neuron-like nets due to its high-speed memory, see Grometstein, *MIT Lincoln Laboratory: Technology in Support of National Security*, 455 ff..

[57] Sutherland, "Sketchpad: A Man-Machine Graphical Communication System," 8.

city could be fabricated and duplicated. Moreover, because of its coded nature, the resulting plan is effectively a modular design; if a designer wants to make some change she can simply edit the data coordinates and redraw the plan. And because the raw data is portable and unambiguous code—rather than a visual, mimetic sketch—communicating and storing the design avoids the introduction of compounding errors.

Like the *Descriptio*, Sutherland's Sketchpad was also an experiment in portable, precise, and unambiguous design. Because Sketchpad was a new kind of design—fundamentally notational—new capacities and modes of interaction were needed for its use. Sutherland developed three novel and significant design capacities for Sketchpad: "subpicture," "constraints," and "definition copying." The subpicture capability was a modular way of associating arbitrary "symbols" to a drawing, which could be combined to create more complex pictures. The constraints capability related atomic parts in a computable way, establishing relationships between lines, points, and circles (e.g., the system recognized when two lines were connected, so that changing a vertex would move both lines in response). The definition copying capability permitted building complex drawings from combinations of simple atomic constraints. There were 17 different kinds of atomic constraints, and together these enabled rough sketching of a shape that could later be refined by copying and editing explicit constraints. These modular capacities permitted easy and unambiguous reorderings, in much the same way that Alberti had explored in a preliminary way hundreds of years earlier.

10.2.2 Codes and secrecy

Playing on the title of Kandinsky's book *Point and Line to Plane*, in ".-/" Gaviria continues his investigation of ciphertext and language. In this work Gaviria transcribes Kandinsky's book into Morse code. The transcription uses the typographic period, hyphen, and slash (hence, ".-/") for a Morse code substitution "cipher." The formal effect is similar to Gaviria's "A Mathematical Theory of Information," ultimately reducing the work to encrypted text. Most curiously, Gaviria's choice to replace the timing sequence of Morse code transmissions with the typographic slash ("/") is a visible performance of "time axis manipulation." Time axis manipulation is the ability to manipulate one of the most basic experiences of human existence, the irreversibility of the flow of time.[58] What makes media technology like Morse code so special is that time

[58] Krämer, "The Cultural Techniques of Time Axis Manipulation," 96. See also chapter seven.

itself becomes a variable that can be manipulated. This manipulation of time is concretized and made visible in ".-/".

Gaviria's ".-/" makes the time axis manipulation visible in the medium itself. In "real-time" Morse code, the transmission timing is set by the sender's "fist" (the frequency and way in which the key or bar is pressed, comprising a "signature" or sorts). Typically, typographical depictions of Morse code transmission elide this important feature, replacing the steady rhythm of dits and dahs with empty space when written on the page. Gaviria elects to show the temporal gap—the time axis—with a slash, thereby revealing the manipulation of the code transcription.

"Beyond Black" (2010) (figure 10.5) appears innocent—a shiny black panel that reflects the image of the viewer. From this perspective, "Beyond Black" has narcissistic appeal as a reflection of the human viewer. Unbeknownst to the viewer, however, "Beyond Black" is actually a nanoscale grid—an order only perceptible to humans with the aid of technology. Like many of Gaviria's works, "Beyond Black" invokes a secret world, but in this case, order is hidden in plain sight. Presciently, "Beyond Black" shows that in a post-Snowden world, we live in a world of open secrets, where the hidden lies in plain sight.[59]

[59] See chapter twelve for a further exploration of the political salience of the "open secret."

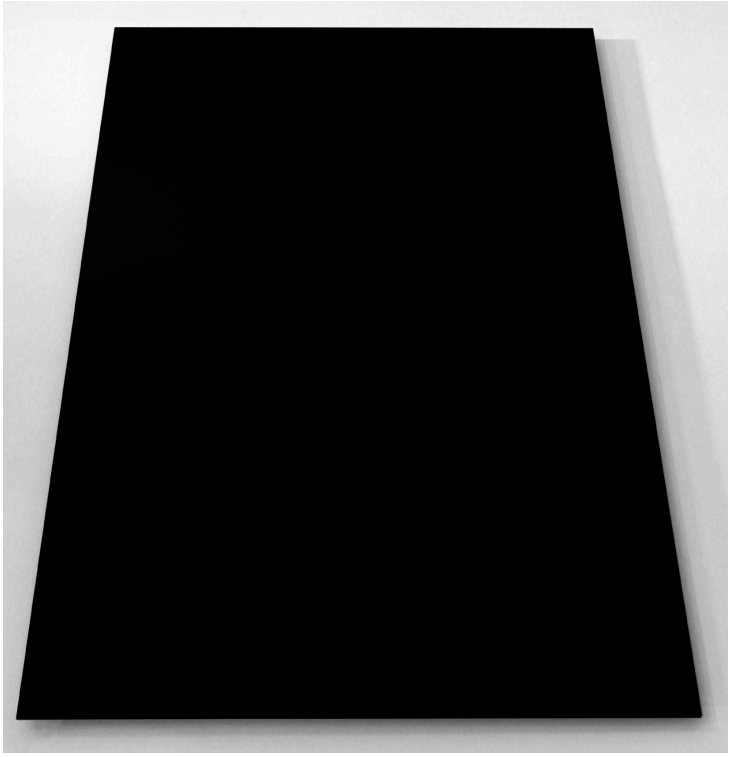


Figure 10.5: "Beyond Black."

"Beyond Black" can be compared to the ultimate secrecy system, the highly classified NSA BLACKER encryption network communication system. The BLACKER programme is a system of encryption technologies and networking infrastructure that was designed to replace aging systems used on top secret military networks. Up until the late 1980s, for intelligence agencies, there were two worlds: red and black. Red is open and informative—plaintext. Black is closed and seemingly meaningless—ciphertext. Gaviria's "Beyond Black" explodes this dichotomy, suggesting that there are codes and orders more black than black, or, blacker. BLACKER was developed to be exactly this, and named as such—BLACKER is more black than black, or beyond black. With this connection in mind, I will describe how the BLACKER project relates to its predecessors—the merely "black" systems developed with the early Arpanet. More than just a chance coincidence of related names, Gaviria's work compels us to investigate these black sites to better understand our point of view, and our political relationship to these technologies.

The NSA BLACKER project was borne out of research in a red and black world, originating from the first system of encryption developed for the

Arpanet (which later became the Internet), the Private Line Interface (PLI).[60] As I explored previously with Fidler, the PLI system was intended to provide link-level security for military networks, necessary since these networks were "open" to a range of interconnections, and connected computers without security measures built in. When its first official message was sent in 1969, the Arpanet had no security provisions. Through consultation with the NSA, and driven by a need for securing military networks, this omission was quickly addressed. By the second quarter of 1973, research had begun on security aspects for the Arpanet. At this point much of the core functionality of the Arpanet was already developed and in use, and the network already connected international partners.

The PLI used a SUE minicomputer in conjunction with a military KG34 encrypting/decrypting machine, which together would appear to the Interface Message Processor (IMP) as a "fake" host. Through its connection with the IMP, the PLI created secure subnetworks within the broader Arpanet. By 1976, Bolt, Beranek and Newman (BBN; the organization hired to build much of the Arpanet) had successfully built and deployed PLI units, and by 1980 they were deployed on the NSA's Community Online Intelligence System (COINS) network.[61] The PLIs were later to be replaced by Internet PLIs (IPLI), but the IPLI did not see wide deployment.

The original IMPs were responsible for addressing and routing messages across inter-networks, as well as taking care of the complexities involved in error correction and performance monitoring, and packet construction (the IMP was a "store and forward" system that buffered bits into complete packets). Later versions of the IMP system, such as the High Speed Modular IMP (HSMIMP) and PLI, added functionality and improved performance. In available documentation, discussion of the PLI first arises in the second quarter of 1973; however, even from this early stage of planning the PLI was already understood to be part of the IMP successor project, the HSMIMP, which was later called "Pluribus." In the first quarter of 1974, BBN had produced their first set of Pluribus IMPs (without security features), although they were still performing debugging and had not yet delivered the machines.[62] Work continued on the development of Pluribus IMPs for satellite and secure applications. At this point, BBN had resolved the architectural questions

[60] Portions of this research have been previously published in DuPont and Fidler, "Edge Cryptography and the Co-Development of Computer Networks and Cybersecurity."
[61] Elsam, "COINS II/ARPANET: Private Line Interface (PLI) Operations Manual."
[62] "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 5."

remaining for the secure PLI system (as an offshoot of the Pluribus), opting for a conservative design that placed the encrypting unit (the "KG" unit) in series between two PLI units, one "red" (plaintext) and one "black" (ciphertext), housed in a single TEMPEST-approved housing (see figure 10.6).[63]

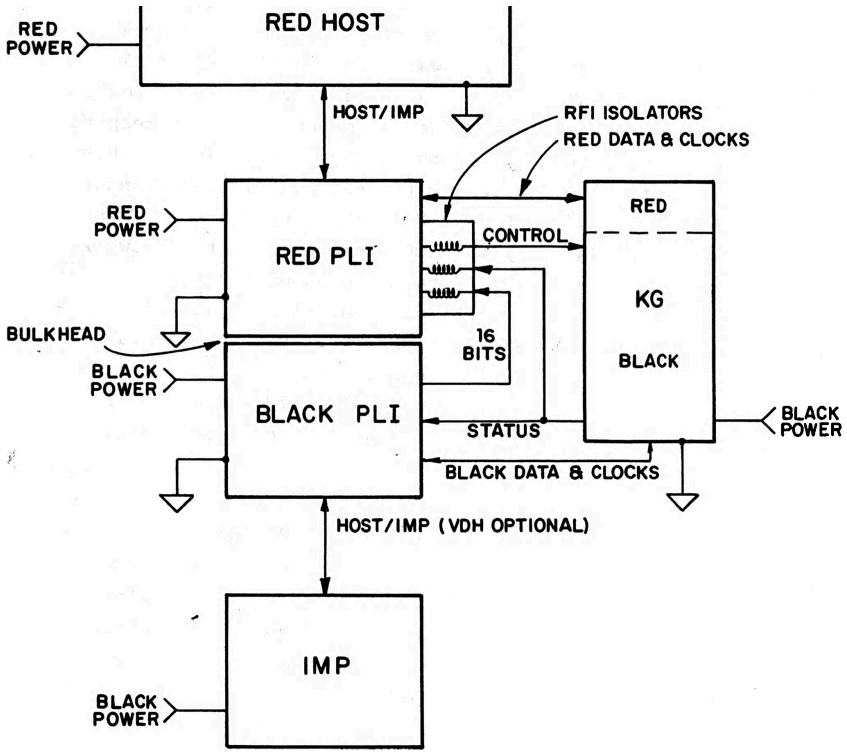


Figure 10.6: Private Line Interface configuration.[64]

Encryption and decryption for the PLI was performed by the KG-34. The KG-34 is a cryptographic device in the KG-30 family, which is still classified and therefore little is known about its design and operation.[65] However, given what is known about available cryptographic technology from the time of the

[63] TEMPEST is the term given to methods of securing electronic equipment from accidental electromagnetic radiation. During the Second World War it was discovered that the Bell 131-B2 telephone "mixer" emitted radiation (detectable on an oscilloscope across the room) each time the encrypting "stepper" advanced. By the 1950s and 1960s these accidental emissions were operationalized by intelligence-gathering organizations and led to strict requirements designed to frustrate eavesdroppers. Today, cryptanalytical techniques that take advantage of electromagnetic radiation (which are extremely common in consumer products) are known as "Side Channel Attacks."

[64] "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 5," 7.

[65] The hardware interface is based on the NSA CSEEB-9B specification, which is also classified; see "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 7," 25.

KG-34 (which was already considered fairly old), it is likely that the KG-34 was a linear shift register that encrypts by performing logical XOR operations on plaintext and key data. It is known that the KG-34 unit was manually keyed (and rekeyed as needed) by authorized personnel who accessed the "permuter boards" inside the KG unit.[66] PLIs on both sides of the network needed to use identical keys for corresponding message encryption and decryption, so keying had to be done in sync. Thus, the KG-34 performed the crucial encryption and decryption steps, while the PLI took care of routing and addressing tasks for message transmission across the inter-networks.

A major missing feature of the PLI was key distribution. Since each PLI was manually keyed, there was little flexibility in configuration, and the rekeying process was labour intensive and less secure than automated or automatic options. In the late 1970s BBN embarked on the Black/Crypto/Red (BCR) project, an encrypting/decrypting device that would work on TCP/IP internetworks (the PLI worked only on virtual subnetworks). According to Steve Kent,[67] the BCR was developed between 1975 and 1980 by Collins Radio or Rockwell, under DARPA funding. The BCR operated with TCP/IP and used the first National Bureau of Standard's certified DES chips, keyed and authenticated by an automated key distribution center (the same model later adopted by BLACKER). By 1980, BCR was undergoing substantial performance testing, and then shortly thereafter shelved. DARPA continued developing DES-based networks through the early 1980s.

Next, the IPLI was implemented as an operational tool for inter-network secure communication in the model established as workable by BCR. BBN developed the IPLI to use TCP/IP and a newer encryption/decryption device (the KG-84), but was still manually keyed.[68] The IPLI was intended as a backup program, funded by DARPA and DCA, in case the more ambitious, multi-level security BLACKER program was delayed (which would cause issues for the new Defence Data Network). BLACKER was indeed delayed, and some IPLIs were deployed in the mid-1980s, but only briefly, and without wide deployment.

Finally, BLACKER was, at least briefly, implemented on the Defense Data Network (DDN) before it was transformed into NIPRnet, SIPRnet, and JWICS. BLACKER was structurally similar to BCR, and thus structurally

[66] Elsam, "COINS II/ARPANET: Private Line Interface (PLI) Operations Manual," 26.
[67] "Network Encryption - History and Patents."
[68] Ibid.

similar to the PLI, in that the cryptography was implemented at the edge—primary in design, but functionally outside of the switches.

By the time BLACKER was deployed, however, the world had changed. Public key cryptography had been publically available since the early 1980s, and had been demonstrated to be robust. Just as the IPLI removed the need for individual keying by creating key distribution centers, with their own security requirements, public key cryptography removed the necessity for key distribution centers altogether by allowing users to engage in secure communication without exchanging keys in advance. Despite the widespread use of public key cryptography for commercial applications, the more conservative choice, adopted by security agencies, is to use traditional cryptography implemented at the edges. BLACKER remains a black site, historically opaque, but emerged out of a world of red and black. BLACKER, however, like Gaviria's "Beyond Black," creates a world more black and black, which throws up new social and political challenges.

❦

In this chapter I showed how social, philosophical, and aesthetic studies of order can reveal a variety of insights about ciphertext. Studies of order have ranged from those typically associated with cryptography (Shannon's measurement of Markov chain probabilities), to the physical sciences (chaos theories), and the growth of the mathematical study of combinatorics (Leibniz's *Dissertatio* and his calculating and enciphering/deciphering machines). In an effort to show how ciphertext does not need to be so narrowly focused on the traditional measures, I introduced Lorand's general account of order that she developed for aesthetic measurement. Using Lorand's account of order I argued that ciphertext is a complex, qualitative (binary), necessary, and lawlike kind of order that is perspectival according to some (often hidden) ordering principle. This interpretation implies, however, that ciphertext is always striving towards otherness, unlike many other kinds of order. The vector that plaintext travels towards the otherness of ciphertext complicates our epistemological grasp on its ontological status.

To more fully investigate how ciphertext complicates the onto-epistemological picture I introduced the work of new media artist Andrés Ramírez Gaviria. As a case study, Gaviria's work exemplifies how ciphertext, and other similar codes, can shift towards otherness by locating themselves "between interpretation and representation." In addition to the aesthetic qualities of his artwork, I interrogated the implied histories of his art subjects. The history that lies behind Gaviria's work reveals how a variety of ordering

principles intersecting with the development of ciphertext have been deployed. This history includes the development of human-computer interactions for the purpose of military command and control, as found in the project of notational ("computer") assisted design, from Alberti in the sixteenth century to Sutherland in the twentieth. More presciently, Gaviria draws out a complicated social relationship to ubiquitous codes and the development of cybersecurity technologies. The history of the NSA BLACKER communications security program grew out of earlier attempts at encrypting Arpanet traffic, using the Private Line Interface set of technologies. Gaviria alludes to this history, a history of the 1970s and 80s when the world was open and closed, or "red" and "black," and draws a comparison to our present situation—strong, ubiquitous cryptography that is either black or BLACKER.

Kittler claimed that cryptography defies interpretation and only permits interception, which also suggests that between forms of representation and interpretation the ordering principles we can understand and control no longer exist.[69] In the place of interpretation, we have developed ciphertext optimized for algorithmic transmission. Unlike other kinds of algorithmic transmission—often too fast or too numerous to comprehend—ciphertext works by ordering plaintext to create a sense of otherness. One might worry that with all these technologies producing relationships of "other," what does this imply for literature, and indeed language itself? As I explore in the next chapter, with no way to speak, through so many cryptographic technologies, perhaps, only silence remains.

[69] Kittler, *Gramophone, Film, Typewriter*, 263.

11
Silence

> *The dispatch-scroll is of the following character. When the ephors send out an admiral or a general, they make two round pieces of wood exactly alike in length and thickness, so that each corresponds to the other in its dimensions, and keep one themselves, while they give the other to their envoy. These pieces of wood they call "scytalae"[σκυτάλη].*[1]

> *It was the Spartans, the most warlike of the Greeks, who established the first system of military cryptography. As early as the fifth century B.C., they employed a device called the "skytale," the earliest apparatus used in cryptology and one of the few ever devised in the whole history of the science for transposition ciphers.*[2]

In the history of cryptography it has long been said that the first cryptography device was the Spartan *skytale* (σκυτάλη). This has been the orthodoxy for over a thousand years, and even David Kahn's field-defining work *The Codebreakers* makes this claim, as do many introductory texts on the history of cryptography today. However, over the last few decades this orthodoxy has been called into question by specialists in classical philology, leading to the demotion of the *skytale* on grounds that it is insufficiently secure to be considered in any way cryptographic. The *skytale*, it seems, is no longer a proper part of the solar system of cryptological devices. I question this demotion, not because I feel that the *skytale* is such an excellent technology, or that I want the Spartans to maintain their position in the historical canon of cryptology. Rather, a proper understanding of what the *skytale* was, and how it was actually used, helps to explain important and fundamental aspects of cryptography more generally.

I argue that the *skytale* was used to establish and maintain silence. Silence, thus, emerges as an important, if forgotten, positivity for cryptography. This argument is not based on the philological record of the *skytale*; rather, it is based on known social and political facts of the Spartan people and their modes of communication and discourse. The Spartans were famous for their brevity of

[1] Plutarch, "Lysander," 285§ 19.
[2] Kahn, *The Codebreakers*.

speech and positive use of silence (we get the epithet "laconic" from the name of the region of Lacedaemonia, where the administrative capital was the city of Sparta). This narrative problematizes our traditional conception of cryptography as a technological apparatus used for "information" secrecy. The narrow, anachronistic conception of cryptography as *essentially secret* has led philologists to rash conclusions. Indeed, aligning silence and ciphertext problematizes the assumed relationships between language, writing, and code, and begs questions about the ontological status of ciphertext. Since ciphertext is grounded in silence, we must also understand what kind of silence applies to ciphertext. Silence is here understood as a positive force that stands in an important relation to verbal language. Of the various possible forms of silence, ciphertext seems to be a kind of "deep silence" that is pregnant and originary. In this regard, ciphertext is a particularly interesting example of deep silence, since before the act of decryption, the source is literally unknown and exists as potentially any text. Ciphertext is the positive and originary ground of the plaintext that ultimately (but only potentially) results.

11.1 THE FOIL: THE *SKYTALE* IS NOT A CRYPTOGRAPHIC DEVICE

It is not clear how the *skytale* originally came to be associated with cryptography, but this view has long been the orthodoxy. The cryptographic operations of the device are described by Plutarch in *Lysander*, one of the primary resources for information about the skytale:

> *Whenever, then, they [the Spartans] wish to send some secret and important message, they make a scroll of parchment long and narrow, like a leathern strap, and wind it round their "scytale," leaving no vacant space thereon, but covering its surface all round with the parchment. After doing this, they write what they wish on the parchment, just as it lies wrapped about the "scytale;" and when they have written their message, they take the parchment off, and send it, without the piece of wood, to the commander [in the field]. He, when he has received it, cannot get any meaning of it,—since the letters have no connection, but are disarranged,—unless he takes his own [matching] "scytale" and winds the strip of parchment about it, so that, when its spiral course is restored perfectly, and that which follows is joined to that which precedes, he reads around the staff,*

and so discovers the continuity of the message.[3]

As is clear from Plutarch's description, the *skytale* is either the wooden rod or perhaps the entire device. Indeed, σκυτάλη was a relatively common Greek word with multiple meanings, the most prominent being simply a baton or rod. The measure of security provided by the skytale of Plutarch's description could not have been very great. Once the operating principle was discovered (a strap is wound around a particularly-sized rod), the effort required to cryptanalyse the message would be minimal. In fact, I imagine that the tolerances of such a system would be so loose that a rod of any reasonable size would get the message at least mostly decrypted. Several authors have argued that because the *skytale* would not have been effective for maintaining secrecy, it could not have been used for cryptographic purposes. Such an argument requires only a little imagination and the working assumption that the Spartan people were not manifestly stupid. Reasonable expectations, and a strong argument.

But Plutarch's description is not the only we have of the *skytale*. In fact, there are nine descriptions of the *skytale* in Greek antiquity, and based on this philological evidence, Thomas Kelly concluded that not a single one of the descriptions point to the conclusion that the *skytale* was a cryptographic device used for secrecy.[4] This view was independently corroborated by Stephanie West.[5]

The first recorded use of the word "*skytale*" is from Archilochus, sometime around 650 BCE, who described it as such: "Like a grievous message stick [skytale], thou son of a Herald, I will tell thee and thine a fable." With only a fragment remaining, the meaning is opaque and there is no suggestion that the *skytale* was a Spartan invention (a view that came into existence later). Based on scholarship on the development of early scripts, West moots the idea that Archilochus may have intended the *skytale* to draw attention to the *written form* of the message—*à la mode*—since Spartan writing was so rare.[6] West ultimately rejects this argument, however, instead arguing that the *skytale* was "a relic of the old oral culture."[7] The stick, West suggests, may have been used for

[3] Plutarch, "Lysander," 285 § 19.
[4] Kelly, "The Myth of the Skytale."
[5] West, "Archilochus' Message-Stick." West's article was published a decade prior to Kelly's publication in *Cryptologia*, but Kelly notes that his publication built on a book chapter published four years prior to West's article. And either way, Kelly points out that both of these contributions came a hundred years after J.H. Leopold's article "De Scytala Laconica," which had already assembled most of the same evidence and came to the same conclusion.
[6] Ibid., 43.
[7] Ibid., 44.

authenticating a messenger (by carving matching notches in both halves of a split stick), or used as a mnemonic aid (like tally sticks).

Next, circa 470 BCE, the *skytale* is mentioned by the poet Pindar.[8] The description is again opaque, but he described a messenger carrying a *skytale* from the Muses, alluding to Archilochus' earlier description. Then circa 400 BCE, Aristophanes linked the *skytale* with the Spartans for the first time, in *Birds* and *Lysistrata*. In *Lysistrata,* the *skytale* stands in for a messenger's erect penis, and the receiving king responds with his own *skytale.* (Aristophanes' fictional story describes an effort by the women of Sparta and Athens to end the Peloponnesian War; the women had been engaged in a sex strike to motivate the men to end hostilities. Therefore, foreign exchanges may have involved an unusual number of rods.) Around the same time as Aristophanes' story, Nicophon mentioned the *skytale* again, but the fragment is once again opaque in meaning.

In the same context, Thucydides wrote a history of the Peloponnesian War that mentioned the Spartan *skytale* (circa 411 - 395 BCE). Xenophon then picked up the history where Thucydides left off, writing the history up to 362 BCE. Both described the *skytale* as a Spartan communication device. But, according to Kelly, it is telling that the work entitled "On the Defense of Fortified Positions," which dedicated a tenth of its length to known systems of steganography (information hiding) and cryptography, did not mention the *skytale*. Kelly finds this omission by such an informed author a damning critique of the argument that the *skytale* could have been a cryptographic device.

Circa 400 - 330 BCE, Ephorus mentioned the *skytale*, which was preserved in Diodorus Siculus's account circa 60 - 30 BCE. This account associated the *skytale* with a kind of Spartan tally stick, used for accounting and identification, but again there was no mention of the use of the *skytale* for cryptographic secrecy. Circa 371- 287 BCE, Theophrastus mentioned the *skytale* in a small fragment on Spartan politics; he wrote, "therefore [the magistrates] conduct the examination in this way with a skytale and, after the examination, they call out the others at the proper time." The meaning is again somewhat opaque, but Kelly concludes that there is no mention of cryptographic secrecy.

At this point, Greek culture spread widely throughout the region under the reign of Alexander the Great (356 - 323 BCE), and the description of the *skytale*

[8] All further philological references and quotations regarding the *skytale* are from Kelly, "The Myth of the Skytale."

appears to change.[9] The Greek Apollonius of Rhodes (via Athenaeus, circa 200 CE) alluded to Archilochus' first description of the *skytale* in his "On Archilochus," but by this point the *skytale* was firmly established as cryptographic in the minds of these authors. Plutarch, another Greek writing circa 50-120 CE, provided the definitive description we saw in the epigraph to this chapter. From this point onwards, several Roman authors mention the *skytale* (some with and some without any clear sense of its use for secrecy), including the Roman Aulus Gellius, circa 180 CE, who provided a full description in line with Plutarch's.

The philological evidence presented by Kelly and West is, in my mind, conclusive. The *skytale* was not a cryptographic device used for secrecy. However, this argument does not imply that the *skytale* was in no way a cryptographic device. The assumption Kelly and West make (as do all contemporary authors), is that cryptography can be narrowly defined in terms of secrecy (such a definition is rarely explicitly made, however). This assumption is anachronistic: a backwards projection of late modern notions of "information secrecy" largely derived from military contexts (indeed, the language used to describe cryptography today is modern and militaristic—using the terms of "attack," "intercept," and so on, to characterize all forms of cryptography). Even by Alberti's day, a full thousand years after the Spartans, cryptography still retained a host of non-secret associations (writing, print, memory), as seen most notably in Alberti's explicit discussion of the printing press in relation to his cipher wheel.[10] Modern authors have missed these connections, preferring instead to think that these unexplainable functions are part of some other unknown category of technology. I argue that the *skytale* was in fact a cryptographic device, just not a cryptographic device used for purposes of secrecy.

My argument is not based on philological evidence, which is scant and problematic anyways. Rather, I offer a conceptual reconstruction that problematizes the existing categories, challenging the traditional alignment between cryptography and secrecy. I argue that the *skytale* was used to establish and maintain silence. This description of cryptography points to deep (dis-) connections between ciphertext and language.

---

[9] Consider, also, Kittler's argument that cryptography requires a developed communication and bureaucracy system, which is why he believed cryptography was invented by the Romans. See Kittler, "Code," 41.

[10] In *De Cifris* (1466). See chapter three for a full discussion of the relationship between the printing press and cryptography.

11.2 THE ARGUMENT: THE *SKYTALE* IS A CRYPTOGRAPHIC DEVICE, FOR SILENCE

Metaphorical descriptions of cryptography often invoke a kind of semantic family of terms: crypt, cover, lock, hidden, veil, and silence. These metaphors hold clues to the ontological status of cryptography, but their ambiguity hinders as much as it helps. It is not clear what connects the items in this semantic family of terms, or if the connection is essential or a "family resemblance." And to the extent that the metaphors pick up on distinct characteristics of cryptography, what are the positive differences? Before I turn to the ontological and phenomenological characterization of silence required to answer such questions, I describe how the *skytale* was used to establish and maintain silence in Sparta. Only then will the path be clear to show how ciphertext can be silent.

The Spartans were a famously silent people, in sharp distinction to the garrulous Athenians (who provided most of the written record we have of Spartans). Intuitively, this characterization suggests that silence played a large and positive role in Spartan life, and that techniques for establishing and maintaining silence would have been prevalent. It does not seem hard to believe that such a culture would have developed a specialized technology to serve this important cultural and political end.

There are, however, methodological challenges that make this a troublesome argument. Compared to the Greeks, who left voluminous written records, very little is known about Spartan society. What is known comes from material (archeological) records and written descriptions by their enemies and exoticizers. It should be expected that written descriptions will exaggerate and pervert the truth, even if they do contain a kernel of truth. And so, if the *skytale* really was a Spartan device, a similar paucity and conflict of description should be expected (this does seem to be the case with the philological record). To make matters worse, the topic of silence, which I am proposing as the key function of the *skytale*, is unlikely to appear with much sophistication in written records, since even today, silence is a poorly understood phenomenon, often understood simplistically as the privation of sound. Thus, very little is known about Spartan life, even less about the *skytale*, and the phenomenon of silence in contemporary life is barely understand today, let alone two millennia ago.

Despite these methodological challenges, the use of silence in Spartan life has recently become a topic of scholarship. For example, David argues that Spartan society employed a "restricted code" with a predisposition for minimizing verbal

expression and reducing communication to the realm of the predictable.[11] David reports that "the manipulation of silence in classical Sparta was extremely elaborate and sophisticated."[12] These techniques extended into many aspects of Spartan society, including education, politics, morality, and military life.

From a young age Spartans were taught, and trained, to preserve silence. Like their austere dress, the Spartans used silence to inculcate discipline, self-restraint, uniformity, and conformity.[13] Spartan communication skills maintained a keen sense of when to speak, and when to remain silent, and the proper ratios of each. Spartan youth were encouraged to say nothing at all rather than to make a mistake. The encouragement of silence in education would often be violent and thoroughgoing, especially in the case of an uttered mistake. The tradition for an uttered mistake was to be reprimanded in an oral but non-verbal way—a ritual bite on the thumb by an elder boy tasked with keeping the youth in line.[14] The proper function of silence was to make the youths "sententious and correct in their answers."[15]

In political life, the Spartans differed significantly from their Athenian counterparts. As one might expect, the democratic nature of Athenian politics encouraged open dialogue. Eloquent rhetoric and long speeches were common in the Athenian Assembly. Spartans politics, by contrast (much more authoritarian in structure), vacillated between silence and its opposite—shouting. In the Spartan Assembly, there was an expectation of silence—to provide a "silent majority."[16] To compensate for this silence, however, loud shouting, modulated only by volume for nuance, provided the Spartan "mixed constitution."[17]

As an extension of proper Spartan education, silence was used normatively throughout society. Affect was always regulated in public, which included crying in silence, expressing joy in silence, and especially, bearing pain in silence. Although most of Spartan society had distinct rules for men and women, in the case of silence, women were expected to maintain the same moral and affective regulations.[18] Perhaps as a consequence of so much affective

[11] David, "Sparta's Kosmos of Silence."
[12] Ibid., 118.
[13] Ibid., 119.
[14] Ibid., 120.
[15] Ibid.
[16] Ibid., 126.
[17] Ibid.
[18] Ibid., 130.

and moral regulation through silence, suicide—in silence—was a common part of Spartan society.[19]

The Spartans were most famous for their military conquests, and silence here played a considerable role. The Spartans would use repetitive or silent operations to create group solidarity. As is the practice even today, the military men would often march in silence, or in repetitive chant. To ensure appropriate silence during long marches, the Spartans developed numerous techniques, such as biting one's lip.[20] The quasi-military Spartan "secret police," the *Krypteia*, were trained to use silence in their yearly raids on the *helots*. The *helots* were a subjugated population that were kept enslaved through a legalized "hunting" season that sought rebellious or powerful actors. Stealth and silence was important to ensure surprise.[21] Similarly, the *helots* were often forced to drink wine to cause logorrhea, vice, and foolishness, thereby depriving the helots of silence and moral righteousness.[22] During these episodes of forced drunkenness, the Spartans would sit in solemn, and judging silence—creating a obvious effect of superiority, and ensuring subjugation through silence.

The Spartans also needed to ensure silence during military campaigns, which, I am suggesting, is the specific use case for the "cryptographic" *skytale*. In addition to the practical utility of silence for comradery and stealth, the Spartans (like all ancients) were a superstitious people. The Spartans needed to protect against accidental utterances—even autonomic ejaculations such as sneezes—before engaging in important tasks. Preparation for war was, above all, an important time for Spartans, and the "phenomenon of identifying chance words… as ominous[,] was an occasional arm of diplomacy."[23] The decision of when and if to go to war was often correlated to the reading of a sign, or the accidental utterance of a name (e.g., the Battle of Mycale in 479 BCE was determined by a "bad omen").[24] In addition to the social norms of keeping silent during war preparations, the Spartans would need to ensure that important communications could occur *silently*—avoiding risk of the accidental utterance of a bad omen. Writing would partially accomplish such a task, but transporting sensitive words in plaintext still left open the chance of an accidental utterance (perhaps by an untrained messenger—smart enough to read, but too stupid to

[19] Ibid., 131.
[20] Ibid., 119.
[21] Ibid., 124.
[22] Ibid.
[23] Lateiner, "Signifying Names and Other Ominous Accidental Utterances in Classical Historiography," 36.
[24] Ibid., 41.

know when to remain silent). The skytale carries ciphertext that is not so much "secret" as silent, since it literally cannot be uttered.

This invention must have seemed strange and powerful, since reading from antiquity up until the invention of the printing press was habitually done out loud (with a return to orality in the discourse network 1800, which is maintained today for educating children, but not adult readers). At the time, the idea of writing in silence, and *for* silence, was as foreign as the Spartans themselves. Thus, it seems plausible that the skytale could have been a cryptographic device to establish and maintain silence, but if so, what does this entail for the ontological status of ciphertext? What does it mean for ciphertext to be silent? What is silence?

11.3 Ontological and Phenomenological Account of Silence

> *He sat down in the usual chair and the usual silence fell between them. Normally he felt the silence like a comforting shawl thrown round his shoulders. Silence was relaxation, silence meant that words were unnecessary between the two of them.… But this night[,]… silence was like a vacuum in which he couldn't breathe: silence was a lack of everything, even trust[;] it was a foretaste of the tomb.*[25]

Silence is not just the privation of sound. In fact, according to Max Picard, silence is a "primary, objective reality, which cannot be traced back to anything else."[26] Consider, for example, Doyle's *Silver Blaze*. The character, Sherlock, cracks the case of the missing horse because the stable dog was silent during the night in question.[27] Sherlock intuited that a silent stable dog must have meant the thief was someone familiar, since otherwise the dog would have barked. In the story, silence was *positive information,* that was critical for Sherlock's deduction. Another characterization of the positivity of silence can be found in the difference between muteness and silence. Muteness is privation of sound, a lack, and a deep inarticulateness incapable of signifying performance. For Picard, and Dauenhauer, silence is full, positive, and an expression in its own right. Perhaps without the trouble of sonic noise to get in the way, in fact, these

[25] Graham Green, *The Human Factor* quoted in Dauenhauer, *Silence, the Phenomenon and Its Ontological Significance*, 22.
[26] Picard, *The World of Silence*, 5.
[27] Doyle, "Silver Blaze."

qualities of silence are experienced more forcefully by deaf people, who despite possessing no capacity for hearing, can and do experience silence (sign language depends on this ability).[28] Deaf people have demonstrated a greater sensitivity to the positive logics of silence, being less likely to think of silence as privation.[29] But, the positivity of silence is unlike other kinds of positive experience, since silence occurs in relief. That is, silence must recognize its surroundings. Susan Sontag describes silence by offering a comparison between positivity and its relief: just as there cannot be an "up" without a "down" there cannot be sound without silence.[30] Similarly, in his essays on silence, John Cage writes that "each something is a celebration of the nothing that supports it."[31]

Silence comes in a number of different forms and is not limited by the choice of media. Sometimes silence is *itself* a kind of performance, as when someone is "keeping silent" in protest, disobedience, or pouting. In fact, silence "itself" is linked to purposive human activity, rather than spontaneous or accidental human performance. Here, positivity is a result of the purposeful nature of the act. Without this positive element, the characterization of silence slips into an account of muteness. These purposive human activities, however, are not limited by media, and need not be oral or even sonic in order to qualify as silence. For example, many forms of art literally do not produce sound, and instead appear to engage in silence, such as miming, private reading, painting, and sculpture.[32] In Wassily Kandinsky's *Point and Line to Plane*, silence is linked to the invisible "geometric point," and the "colourless colours" of black and white are called "silent colours" because the "sound" is reduced to a "scarcely audible whispering and stillness."[33] In the case of Kandinsky's art, the expression of silence does not occur in sound, yet his descriptions end up evoking sonic properties because natural language is used for the description, which is so faltering and inadequate for the task of describing silence.

Despite the challenges of describing silence *within* language, silence is most often linked to oral utterance, and we are keenly aware of such silences when they occur. Our acute awareness is due to the fact that speech makes extensive use of silence, requiring periods of silence to form words and phrases.

---

[28] Dauenhauer, *Silence, the Phenomenon and Its Ontological Significance*, 4.
[29] Krentz argues that hearing people cannot experience deafness (in silence) any more than "donning blackface makes a white person African American." Krentz, *Writing Deafness*, 76.
[30] Sontag, "The Aesthetics of Silence," IV.
[31] Cage, *Silence*, 139.
[32] Dauenhauer, *Silence, the Phenomenon and Its Ontological Significance*, 4.
[33] Kandinsky, *Point and Line to Plane*, 25. See also Gaviria's exploration of the silence of *Point and Line to Plane* in chapter ten.

Translators have particular difficulties when facing the translation of silence. So much so, Carson writes, that "silence is as important as words in the practice and study of translation."[34] Carson notes that there are two kinds of silence facing the translator: physical and metaphysical.[35] Physical silence occurs when, for example, a poem of Sappho's inscribed on a papyrus has been torn. For these sorts of circumstances, the translator has an arsenal of representational tools to deal with the challenge—perhaps signifying the silence that results from the caesura with brackets, or textual conjecture. Metaphysical silence, on the other hand, occurs within the words themselves and has a positivity which poses a greater challenge. Some words are untranslatable precisely because of their silence. Carson suggests that in Homer's *Odyssey,* the word μωλν is untranslatable because it is intended to remain silent. In the *Odyssey,* the word is spoken by the gods, and is thus incomprehensible to *Odysseus*. In uncharacteristic fashion, Homer *transcribes* but does not *translate* the word into Greek (Homer usually translates the gods' language).[36] Philologists suggest that the word actually has some vestige of old Indo-European language within it, but the effect Homer intends, it seems, is to let the word "fall silent."[37]

The account so far has only scratched the surface of the complexity and depth of silence, but what is clear is that silence is not a simple privation of sound. Rather, silence is an active performance that stands in relief to its surroundings, constituting a positivity that can be felt and understood by people when silence is paid attention to. And to pay attention to silence is to realize that it is not phenomenologically uniform in kind. Dauenhauer argues that there are three distinct, and not phenomenologically uniform, kinds of silence: intervening silence, fore-and-after silence, and deep silence.[38]

Intervening silence is the occurrence of silence that punctuates words and phrases in discourse.[39] Such silences are important for clarity and meaning, as is clearly demonstrated when a person mumbles in a foreign language. Such speech is incomprehensible to new language learners, who are incapable of parsing words and sentences. Intervening silences are also temporally complex, as the silence appears to go through phases of meaning and function. That is, the intervening silence terminates the initial sound phase, and clears the way for

[34] Carson, *Nay Rather*, 4.
[35] Ibid.
[36] Consider also the relationship between transcription and translation and decryption and cryptanalysis discussed in chapter nine.
[37] Carson, *Nay Rather*, 6.
[38] Dauenhauer, *Silence, the Phenomenon and Its Ontological Significance*, 3–26.
[39] Ibid., 6.

the next. Because of this complex time structure, intervening silence has a distinctive role in marking the sequences of sounds as "mine," "yours," and "anyone's," and so on.[40]

Fore-and-after silence is like intervening silence, in that it opens and closes, but each phase lacks the associated pair (that which is "intervened" between). Complete utterances are surrounded by fore and after silence. Unlike intervening silence, fore-and-after silences are not rhythmically significant. Comparing the two, it seems that after-silence has more impact and positivity than fore-silence. For instance, in a well-crafted expression, if an utterance were to have terminated at a different time the utterance would have lost, not gained, significance. Indeed, after-silence contributes to a "well-crafted unity," which can be used to create anticipatory alertness, or alternatively, alertness that can be "savoured."[41] Aristotle's notion of *muthos*, the idea of mimetic completeness and integrity of art, relates to this after-silence.[42] Misplaced after-silence results in a wrenching experience in art and dialogue. More prosaically, proper use of after-silence means knowing when to shut up. Fore-silence can be important as well, since it contains the "residue" of utterances that have already passed. Knowing and remembering what a person said previously can shape expectations of future discourse. Fore-and-after silence, ultimately, form a pair, and interrelate.

The various kinds of silence are distinct but not mutually incompatible, and the third, deep silence, is at play in all utterances of whatever sort.[43] Dauenhauer divides deep silence into a further three kinds: the silence of intimates, liturgical silence, and the silence of the to-be-said (which is also a kind of normative silence). The silence of intimates has no specific achievement as its primary goals, and in a narrow Shannon-esque sense does not primarily transmit information. In the silence of intimates, as described poignantly in the depiction of the couple in the epigraph to this section, intimates can stand in silence of love, hate, bearing in resignation, and so on. Dauenhauer notes that once the silence of intimates has begun, it is somehow maintained through utterances, but the number and frequency cannot be specified.[44] Liturgical silence is associated with ritual worship, but not all religious experiences or forms of worship entail silence. Catholic and Quaker worship are perhaps the most famous examples of liturgical silence in the West. Quakers, for instance, do not employ this kind of deep silence to enable something further, rather the

[40] Ibid., 8.
[41] Ibid., 10–11.
[42] See chapter three.
[43] Dauenhauer, *Silence, the Phenomenon and Its Ontological Significance*, 16.
[44] Ibid., 17.

goal is to open a space for God's activity.[45] The silence of the to-be-said lies beyond what humans can achieve by their own endeavours. This is a normative and philosophical silence, and linked with tact and good sense. It is a silence "beyond all saying," the silence of the "what-ought-to-be-said" in which "what-is-said" is embedded.[46] The "what-is-said" appeals to the "what-ought-to-be-said" for authentication, and is thus originary of positive utterances.

Dauenhauer concludes by summarizing the four fundamental aspects of silence:[47]

1) Silence in an active human performance that always appears in connection with an utterance,
2) Silence is never an act of unmitigated autonomy, rather:
3) Silence involves a yielding following upon an awareness of finitude and awe.
4) The yielding of silence binds and joins.

All distinct types of silence are reconfigured in ciphertext, but deep silence is most directly employed by the phenomenon of ciphertext. Deep silence is also the kind of silence most clearly favoured by the Spartans (especially for use in educational, disciplinary, and normative functions). While the *skytale* disrupts interleaving silence and fore-and-after silence, it does so only as a by-product of establishing a deep silence. Speaking the message carried by the *skytale* becomes an impossibility, and so the entirety of other non-sonic expressions are disrupted also. The *skytale* literally stands for silence, in a deep, normative way. Thus, the *skytale* is as much a talisman of silence and its multiple meanings, as it is a useful mechanism to establish and maintain silence.

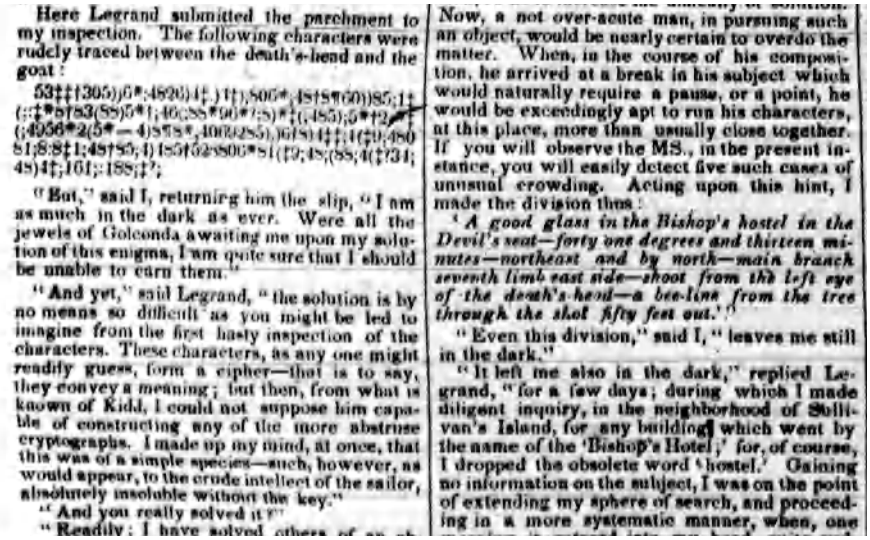
11.4 Silent Ciphertext

Ciphertext is not just "silent" in a metaphorical sense. For the Spartans it established and maintained *literal silence*. And, as described, it is clear that silence is a complex, positive force. So, how does ciphertext establish and maintain silence? Recall (from chapter eight) that cryptography works *on* language, not *through* language. Ciphertext does not use linguistic features and functionality to create silence. Therefore, intervening and fore-and-after silence, which are closely related to the linguistic actions of prosody, rhythm, and mimetic representation cannot be the mechanisms of silence used by ciphertext (but they are disrupted by ciphertext).

[45] Ibid., 18.
[46] Ibid., 19.
[47] Ibid., 24.

Ciphertext is not a linguistic silence because it cannot be spoken. Ciphertext "breaks" the natural alliances of language. In my own personal experience, I first saw this destruction of spoken language—of ciphertext forcibly working on language—in E.A. Poe's famous cryptography story, *The Gold Bug* (1843). *The Gold Bug* is a short story that follows the character William Legrand's discovery of hidden treasure, as told from Legrand's friend's perspective, the unnamed narrator. The story starts with the narrator being summoned to visit Legrand on Sullivan's Island in South Carolina to help find hidden treasure. Legrand was made aware of the hidden treasure initially because he was bitten by a gold scarab-like bug, but after an initial exploration with little success, the narrator leaves. A month later, the narrator returns and their search begins in earnest. The narrator follows Legrand and his slave Jupiter through a number of strange activities, including climbing a tree and dropping the gold bug through a branch. Once the treasure is secured, Legrand explains to the narrator how he uncovered the riddle, which required decrypting a ciphertext message that revealed a (convoluted) description of how to find the treasure.

I did not first encounter Poe's story in the typical way, however. In the original published version (serialized in the *Philadelphia Dollar* newspaper, after Poe won a short story contest), and likely all printed versions since, the ciphertext that Legrande puzzles over was set by its own, in rows of type on the page (see figure 11.1). Such a presentation of ciphertext was quite common at the time, and newspaper readers in Poe's day would have been familiar with a code challenge being printed in the newspaper. Code cracking was a very popular activity at the time, and Poe capitalized on this interest to great effect (*The Gold Bug* was easily his most popular story during his lifetime).



Here Legrand submitted the parchment to my inspection. The following characters were rudely traced between the death's-head and the goat:

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;1‡ (;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:‡ (;4956*2(5*—4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48 81;8:8‡1;48†85;4)485†528806*81(‡9;48;(88;4(‡34; 48)4‡;161;:188;‡?;

"But," said I, returning him the slip, "I am as much in the dark as ever. Were all the jewels of Golconda awaiting me upon my solution of this enigma, I am quite sure that I should be unable to earn them."

"And yet," said Legrand, "the solution is by no means so difficult as you might be led to imagine from the first hasty inspection of the characters. These characters, as any one might readily guess, form a cipher—that is to say, they convey a meaning; but then, from what is known of Kidd, I could not suppose him capable of constructing any of the more abstruse cryptographs. I made up my mind, at once, that this was of a simple species—such, however, as would appear, to the crude intellect of the sailor, absolutely insoluble without the key."

"And you really solved it?"

"Readily: I have solved others of an ...

Now, a not over-acute man, in pursuing such an object, would be nearly certain to overdo the matter. When, in the course of his composition, he arrived at a break in his subject which would naturally require a pause, or a point, he would be exceedingly apt to run his characters, at this place, more than usually close together. If you will observe the MS., in the present instance, you will easily detect five such cases of unusual crowding. Acting upon this hint, I made the division thus:

'*A good glass in the Bishop's hostel in the Devil's seat—forty one degrees and thirteen minutes—northeast and by north—main branch seventh limb east side—shoot from the left eye of the death's-head—a bee-line from the tree through the shot fifty feet out.*'

"Even this division," said I, "leaves me still in the dark."

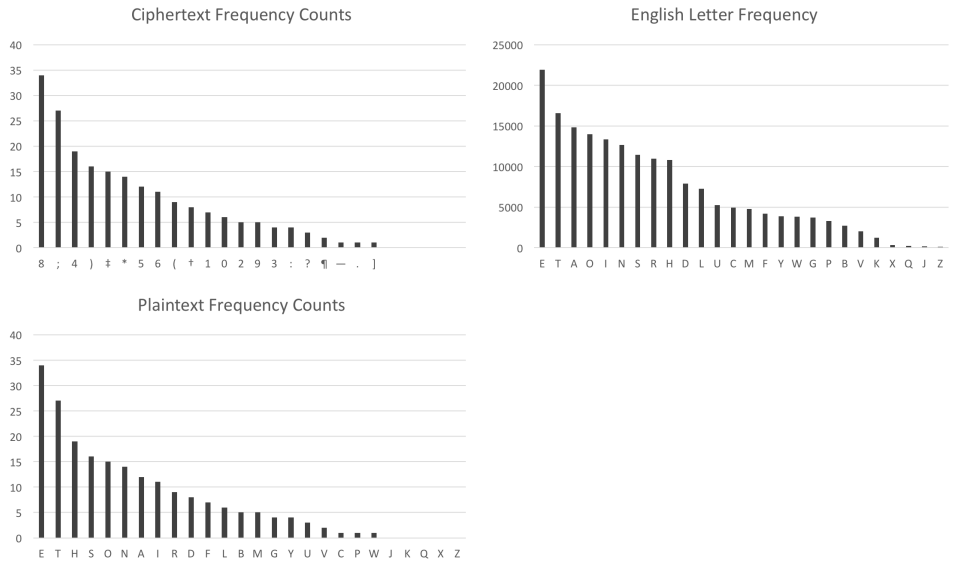
"It left me also in the dark," replied Legrand, "for a few days; during which I made diligent inquiry, in the neighborhood of Sullivan's Island, for any building which went by the name of the 'Bishop's Hotel;' for, of course, I dropped the obsolete word 'hostel.' Gaining no information on the subject, I was on the point of extending my sphere of search, and proceeding in a more systematic manner, when, one

Figure 11.1: Ciphertext section from first publication of Poe's *The Gold Bug* in Philadelphia Dollar newspaper.[48]

Poe took himself to be a cryptographer and codebreaker of considerable ability, and included the literal ciphertext in *The Gold Bug* as a challenge and bit of multimedia fun for his readers. The message was encrypted using a monoalphabetic substitution cipher, which could be cryptanalysed through educated guessing and/or some paper and pencil analysis. Due to the simplicity of the encrypting method, traces of the plaintext show through in the ciphertext, as direct one-for-one letter substitutions (e.g., A=5; 3=G). A frequency analysis shows a very characteristic curve mapping close to English letter frequencies (see figures 11.2, 11.3, and 11.4).[49] Although by no means a complex form of ciphertext, "reading" the ciphertext would be a fruitless exercise. But in a weird twist of fate, this is precisely how I first encountered Poe's ciphertext.

[48] Poe, "The Gold Bug."

[49] Cf. chapter eight's discussion of frequency analysis for cryptanalysis. The decrypted text with punctuation added is: "A good glass in the bishop's hostel in the devil's seat, twenty-one degrees and thirteen minutes northeast and by north, main branch seventh limb east side, shoot from the left eye of the death's-head a bee line from the tree through the shot, fifty feet out."



Figures 11.2: Ciphertext frequency counts; Figure 11.3 Plaintext frequency counts; and Figure 11.4: English letter frequency; from Poe's *The Gold Bug*, compared to typical English letter frequency.[50]

The first time I encountered *The Gold Bug* was through an audio recording, listening to a "book on tape," as was once the medium. For most of the audio recording, Poe's story unfolded like any other version. When it came time to represent the ciphertext, however, the producers of the audio version had a difficult decision to make. The ciphertext sits on the printed page like a wall of text—strange symbols arranged in an orderly but ultimately arbitrary fashion (until the ciphertext is cryptanalysed there is no reason to think that it is to be "read" left to right, top to bottom, or any other particular way). It might be thought that the producers faced the same issue as Carson, when she translated the torn pieces of papyrus containing Sappho's poetry. The ciphertext does create a caesura, like a ripped page. But if it was as simple as this, the producers could have used an editorial marker of some kind, perhaps breaking the fourth wall of the audio performance and telling the listener directly that the page of the book contained ciphertext. This would have been an unsatisfying approach, however, because the silence of ciphertext is more substantial and positive than this. The silence of the ciphertext is internal and essential, and after all, not physically missing like Sappho's poetry. Poe *intended* the reader to see the ciphertext, and probably expected the reader to try her hand at cryptanalysis. Poe made sure that the ciphertext was printed correctly, and was real, not just

[50] English letter frequency is based on corpus of 40,000 words; corpus data from: http://www.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html.

some aesthetic effect (as was the case with the electronic art noire book, *Agrippa*, and its self-destructing encryption effect).[51] Instead, like Carson's *non-translation* of Homer's word μωλν, the silence of Poe's ciphertext has an essential positivity. The producers of the audio version, however, decided the least problematic approach was to have the narrator speak the ciphertext. And so, the narrator of the audio recording of Poe's *The Gold Bug* spends a minute slavishly voicing—*viva voce*—the entirety of the ciphertext.[52]

The result is not silence. But, it is also not language or oral representation—and nor could it have been! The very act of voicing ciphertext reduces language to a farce—a minute of slavishly reading code is humorous, yet the narrator trudges through. The ciphertext *ought* to have remained silent, but the *audio* recording denied such a possibility, so the ciphertext lashed back. In the end, after hearing a voicing of the ciphertext, the listener is not much better equipped to understand the story, and no closer to cryptanalysis.

Ciphertext works on language by breaking its natural alliances, but the effect is not total or binary. Pig Latin, for example, is a kind of substitution cipher that can be spoken. The "security" of Pig Latin is low, and it leaves many parts of speech intact. Most importantly, Pig Latin binds consonants with vowels, which makes voicing possible.[53] Or consider how by capitalizing on this quirk of spoken language the Roman Augustus was able to use a form of encryption that replaced vowels with consonants, so that when spoken aloud it would end up producing an unpronounceable jumble.[54] Another example of the continuum between silent ciphertext and language can be found in Jonathan Swift's "Latino-Anglicus."[55] Swift developed a strange kind of "cipher" that uses real Latin words in nonsense fashion that can only be deciphered if reconstructed in silent text. A historian of Swift, Paul Child, argues that Swift's cipher "requires a reading and not a sounding out" because the proper Latin pronunciation obscures the English plaintext. For instance, if spoken with proper Latin

[51] See chapter five.
[52] Consider also an emerging work of new media artist Andres Gavirez Ramírez (I explored some of his work in chapter ten). Upon seeing an early draft of this chapter, Ramírez informed me—completely without prior knowledge to my experience with Poe's story—that he had been at work producing an audio recording of a previous work of his, the "*Mathematical Theory of Communication,*" which is a transcribed version of Shannon's *Mathematical Theory of Communication*. Ramírez's version of Shannon's MTC is transcribed to increase information density, effectively through the use of an encryption algorithm, which renders the result unreadable (comprised of jumbled letters, like Poe's ciphertext). And so, when recorded orally (on a long playing vinyl record, no less), Shannon's MTC becomes a seven hour long farce.
[53] See chapter nine for another discussion of Pig Latin as a liminal form of encryption.
[54] Kittler, "Code," 41.
[55] Child, "Cipher against Ciphers."

pronunciation, "I cum here formo ni," the English phonetic recreation, "I come here for money" is not revealed.[56] Like the Spartans, Swift used his cipher "as much from his concerns about dangerous misrepresentations and misappropriations of language as it did from his love of word play."[57]

❦

This chapter revisited the history of the Spartan *skytale* to demonstrate how silence is an important positivity of ciphertext. The Spartans used the skytale to pragmatically establish and maintain silence, an important cultural, political, and military phenomenon for them. I argued that the *skytale* would be especially useful for military planning, when the Spartans needed to ensure that "bad omens" were not accidently uttered, which would be seen as potentially compromising future military campaigns. This specific example of the *skytale* was generalized, to shed light on the complex phenomenon of silence, a positive force in some ways tied to language, and in other ways much deeper with its own positivity and originary force. Three distinct forms of silence were identified, and I argued that ciphertext deploys deep silence. I then offered some examples of how ciphertext works on language to "break" natural alliances in its effort to ensure silence. An audio recording of Poe's *The Gold Bug* was offered as an example of how silent ciphertext works on language, turning any oral performance into a linguistic farce. I argued that the silence of ciphertext is not, however, total or binary. Rather, silent ciphertext admits degrees of its force on language, with some "weak" forms of encryption resulting in only partially silent ciphertext.

Ciphertext is oriented towards silence, and when successful produces a degree of silence. This deep silence is the origin of plaintext, like Derrida's notion of *arche*-writing, it is the ordered textual basis of language.[58] The "what-is-said" appeals to the "what-ought-to-be-said" for authentication, and to the "what-can-be-said" for production. Thus, silent ciphertext is a pregnant and full phenomenon, not a mere privation. Once language becomes ciphertext, it too becomes silent. As more of the world changes from writing to plaintext to ciphertext, this pall of silence threatens to disrupt and violate language. The resulting silence is not necessarily a diminishment, however, but a positivity that produces its own unique concerns and politics, demanding of our attention.

[56] Ibid., 257.
[57] Ibid., 258.
[58] Cf. chapter nine's discussion of the order of ciphertext. See also Derrida, *Of Grammatology*.

12
Epilogue

> I'm a bit skeptical as to whether 'the political' is really a thing. Partly on traditional Marxist grounds, partly because I think certain kinds of technical power may have superseded it even if it existed.[1]

I have argued that cryptography is comprised of three parts, each with their essential and cognate associations. Plaintext is a form of notational writing that has a long history of co-development with writing and computing machines. For a while, these machines attempted to perfect the mechanisation and manipulation of artificial, perfect and universal forms of code. I argued that plaintext necessarily involves the production of representational violence, as part of the process of creating notational unities and identities out of the "natural" world and its languages, and as part of the vector towards potential encryption.

Encryption is a transcription that maintains the notational properties of plaintext, functioning as a memory technology that essentially transmits across time, rather than communicating across space. When paired with a communication mechanism, however, encryption augments the underlying medium in ways that were often thought to be ideal and capable of sending across space without a material medium. I also argued that while cryptanalysis is a necessary possibility, its essential methods are distinct from its dialectical pair, decryption. As per my archeological method, different methods means different ontologies, which means, cryptanalysis is fundamentally linguistic, and distinct from the notational ontology of encryption and decryption. Encryption is a vector that leaps across language, rather than going through it, as it transcribes plaintext into ciphertext. This process bridges two radically different worlds—one knowable (plaintext) and one unknowable (ciphertext). In order to bridge these worlds, encryption makes use of "messengers," which I described through the myths of angels. I used this messenger model to replace the mathematical one that is typically used to describe encryption.

The world of ciphertext is foreign and Other, and even though ciphertext has the appearance of disorder and chaos, I argued that it is in fact a highly-ordered form of notation. Ciphertext is the product of transcription activated through (encryption) algorithms. Because of this highly ordered nature, ciphertext necessarily distinguishes itself from language, especially the oral performance of

[1] Wark, "A Slow Reader's Books of the Year."

language. That is, encryption works on language, not through it, to produce ciphertext that is a pregnant, positive, and originary form of deep silence.

As an archeological investigation, this study activated many surprising alliances, that have seldom received due attention. Moreover, few if any of these issues have been previously put into dialogue with cryptography. While independently interesting, I have attempted throughout this dissertation to expose the fact that, more than any other aspect of the complex artifact we call cryptography today, cryptography is not a neutral technology sitting on the engineer's shelf, as though ready-at-hand, with no history or peculiar conceptual baggage. However, this ready-at-handedness—instrumental rationality—is precisely how cryptography is typically treated today.

Cryptography continues to become more ubiquitous, essential, and potentially problematic. In an effort to highlight some of the contemporary political challenges presented by ubiquitous cryptography, I conclude with an analysis of the rapidly expanding universe of cryptographic "blockchain" technologies, as they have emerged from the digital currency, Bitcoin. Within a few years of its launch in 2009, people realized that the decentralized ledger technology that powers the Bitcoin economy was capable of supporting a much broader range of uses. In the last few years, this has meant that the cryptographic underpinnings of the blockchain system have expanded into new realms of society. This contemporary and quickly developing technology shows that the trend towards broad uses of cryptography, which I investigated previously from a historical perspective, is still ongoing. Cryptography has never been only a communications tool, and with blockchain technologies we can see it expanded in real time into the realms of money, law, and perhaps even politics. As with any technology, there are potential risks and rewards, but as cryptography infiltrates deeper into the social fabric of life, we need to question these changes.

12.1 From Money to Law to Politics

Blockchain technologies have experienced three distinct phases of use.[2] The first phase is characterized by monetary uses—its original application for the Bitcoin protocol. The second phase is characterized by pseudo-legal uses, as with smart contracts, smart property, and decentralized autonomous organizations made possible through Ethereum and other similar protocols and systems. The third

[2] For a slightly different characterization, focusing on the first two phases, of expansion, see O'Dwyer, "The Revolution Will (Not) Be Decentralised.".

phase is still emerging and has grown out of the pseudo-legal framework of the second phase, characterized by direct and overt political activities, such as pseudo-democratic controls (e-voting) and blockchain versions of government services (identity, welfare and state benefits, utilities management, taxation, and so on). To some extent, many of these uses have existed, potentially or in actual use, since the first blockchain protocol. For instance, a blockchain version of e-voting has been possible since the blockchain's inception, yet it still remains on the horizon in terms of actual adoption. And, even though many of these uses have been technically feasible for a long while, they have not necessarily changed the social imaginary.

The first phase of blockchain use needs little explanation.[3] Bitcoin was originally heralded as an anonymous replacement for cash. In this capacity, its pseudonymous designer, Satoshi Nakamoto, drew on the work of Adam Back, who in 1997 designed hashcash to limit email spam.[4] A year later Wei Dai adapted Back's system and proposed b-money.[5] While neither of these systems had yet developed any notion of a blockchain, they had functionally solved most of the issues for digital money (including protections against counterfeiting). The addition of a blockchain made decentralized token authentication possible—using a cryptographic Merkle tree to ensure authenticity of all transactions, back to the very first block. To "mine" new blocks (i.e., mint new money), Nakamoto drew on Hal Finney's reusable proofs of work framework.[6] Bitcoins thus soon became valuable, and were exchanged for other fiat currencies and stored for value, just like cash.

As Bitcoin grew in size and popularity, the gravity of interest for monetary uses has since shifted into financial technology. Early on, the idea of using Bitcoin to settle balances and books for banks and financial organizations was mooted, but due to the extreme price instability of Bitcoin, such exchanges were deemed problematic, even for spot pricing. Instead, as the Bitcoin community

[3] The earliest academic discussions of Bitcoin started in 2011, although with the exception of Maurer, most early academic discussions of Bitcoin tended to be about economic issues or engineering, rather than social scientific or humanistic issues; Maurer, "Money Nutters." In 2013, introduced social scientific and humanistic viewpoints to academic discourse. See Maurer, Nelms, and Swartz, "'When Perhaps the Real Problem Is Money Itself!'"

[4] Back himself drew on David Chaum's Digicash, who invented the notion of a "blind signature," which is an essential cryptographic part of blockchain technology. See Back, "Hash Cash Postage Implementation." and Chaum, "Blind Signatures for Untraceable Payments." For a broader picture of the historical and technical details, see DuPont, "The Politics of Cryptography: Bitcoin and the Ordering Machines."

[5] Dai, "PipeNet 1.1 and B-Money."

[6] Finney, "RPOW - Reusable Proofs of Work."

slowly recognized the power of alternative configurations of blockchain technology, in the form of sidechains, "colored coins," and non-Bitcoin blockchains, interest grew for using blockchain technology as a purely administrative ledger system in finance.[7] Indeed, one of the hottest "startup" uses of blockchain technology today is for financial settlement and clearing. This function grew out of the monetary uses of Bitcoin, and has since been generalized further, leading to the second phase of blockchain use.

The second phase of blockchain use departs from monetary applications entirely, and adds further functional capabilities that are either impossible or difficult to implement in Bitcoin-compatible blockchains. Due to this generalization of the technological underpinnings, many functions became possible, but the preponderance of interest and growth so far has been focused on pseudo-legal uses. Popularized by Ethereum—a leading alternative blockchain organization—smart contracts, smart property, and decentralized autonomous organizations have become fashionable blockchain uses characterizing this second phase.

Smart contracts, smart property, and decentralized autonomous organizations utilize programmatic scripts and tools, which are added to otherwise fairly static blockchains (in the style of a traditional ledger). By adding programmatic functionality, transactions held on a blockchain ledger can change in response to programmed sets of conditions. In the classic smart contract example, if I hire you to do X, upon successful completion of X you are automatically paid Y, as per the original smart contract.[8] Entire decentralized and autonomous organizations, it is imagined, can be run this way: complex rules for company bylaws and (perhaps) operational tasks execute automatically with no need for human intervention. Indeed, the Ethereum advertising graphics make the proposed vision clear, with automated processes (personified as robots) interacting seamlessly with human agents (figure 12.1).

[7] There are numerous configurations of blockchains possible, which may be "pegged" to Bitcoin's value, or independent of it. Similarly, functionally equivalent, compatible, or incompatible blockchains can be created distinct from the Bitcoin implementation. For a discussion of the blockchain's ledger system, see DuPont and Maurer, "Ledgers and Law in the Blockchain."

[8] Determining success criteria of contracts remains a challenge for "real world" applications. One possible solution is the establishment of independent pseudo-legal bodies, sometimes called "oracles," whose sole job is to determine success criteria. One wonders, however, if this pseudo-legal body is not really just an actual legal body, performing a typical legal task.

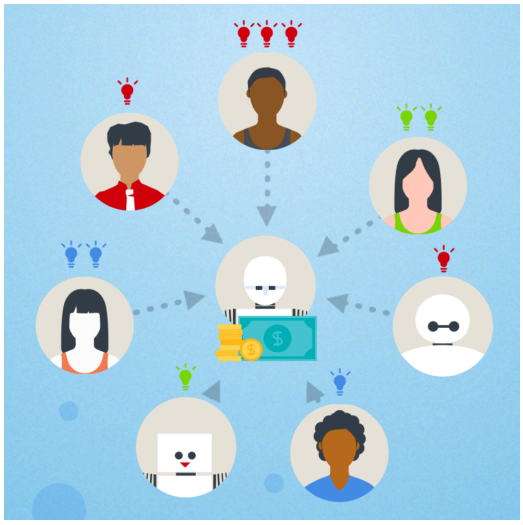


Figure 12.1: Ethereum's graphical depiction of human-machine symbiosis on the blockchain.[9]

One consequence of this shift towards pseudo-legal uses of blockchain technologies is that existing notions of law, and their associated practices, are liable to be replaced or circumvented by cryptographically-secure (and irreversible), automated executions of code. This "code is law" phenomenon has been a persistent worry of legal scholars for decades, stated most persuasively by Lawrence Lessig in his first version of *Code and Other Laws of Cyberspace*.[10] Since Lessig's early characterization, the severity and ubiquity of cryptography has rapidly increased. In fact, not only does the persistence of irreversible and automated code challenge existing legal notions, according to Lessig, it obviates the very category. The snappy phrase "code is law" does not mean code works like law, or that code can or should (or shouldn't) regulate instead of law. Rather, "code is law" means code actualizes or activates—ontologically and temporally—*prior to law*. Lessig uses the example of digital rights management on electronic books: "What if, that is, the software itself could regulate whether you read the book once or one hundred times; whether you could cut and paste from it or simply read it without copying[?]"[11]The important point is that *it doesn't matter* if you have legal rights (or exemptions) to do as you want with the

[9] https://ethereum.org/

[10] Lessig, *Code and Other Laws of Cyberspace*. The argument is repeated in a highly reworked second version Lessig, *Code v2*. However, due to criticism and pressures that he acknowledges in the second version, Lessig shies away from the "code is law" slogan (it occurs only five times in the second version). I think this is a mistake, and I think most commentators failed to grasp the true meaning of the slogan.

[11] Lessig, *Code v2*, 177.

book; if the code prohibits it in the first place, law does not even enter into the equation. The same with smart contracts or smart property on a blockchain.

Today, Wright and De Filippi argue, society is now characterized in a significant way by "*lex cryptographia*." In terms of blockchain technologies, *lex cryptographia* means self-enforcing blockchain contracts "aim to operate free from the reach of regulation," which presents "concrete challenges… to law enforcement,… [and] property rights."[12] If legal scholars are worried about the distortions to law caused by code obviating long-held legal protections, however, it is the third phase of blockchain use, I argue, that is cause for concern for *everyone,* and in many more scenarios and realms of life.

The third phase of blockchain use grows out of the second: from pseudo-legal uses, which often obviate the existing category of law, grows actual and overt political uses. Of course, the blockchain has been "political" since its inception. Like any technology, it has always functioned normatively (non-neutrally), but due to its origins within the cypherpunk community, the blockchain is an unusually polarizing and political technology. Golumbia argues that "Bitcoin is a technology whose social and political functions far outstrip its technical ones;" "Bitcoin appears to be mostly a realization of these political concerns;" and that "Bitcoin is politics masquerading as technology."[13] Specifically, Bitcoin (and by extension, all blockchain technologies) is aligned with right wing, libertarian thought of the most extreme kind. Similarly, like the "code is law" function of the second phase, Scott argues that blockchain technologies are political "replacement systems," which do not augment existing political systems but rather replace them.[14] Of course, not everyone in the Bitcoin or blockchain community holds these political views, but there certainly does appear to be a natural alignment between these views and the design, technological affordances, and uses of the technology.

Paradoxically, despite the desire for unfettered freedom by much of the blockchain community, such technologies may end up actually constraining and controlling individuals in powerful and largely invisible ways. Indeed, as I have argued previously, due to its cryptographic fundamentals, the broadening reach of blockchain technologies may be leading society into a world of control, an effect of the blockchain's ability to order representations. Drawing a distinction between old-fashioned media (television, radio, film) and new blockchain ones,

[12] Wright and De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," 2–3.
[13] Golumbia, "Bitcoin as Politics: Distributed Right-Wing Extremism," 119.
[14] Scott, "Visions of a Techno-Leviathan."

I wrote previously: "algorithmic technologies are able to sort, move, and re-arrange entire populations in ways that mimetic technologies are unable to accomplish."[15] Similarly, Lustig and Nardi argue that blockchain technologies can produce a form of "algorithmic authority;" yet, in their empirical study they found that (perhaps unsurprisingly) members of the blockchain community prefer such algorithmic authority over conventional forms of authority, which they deem untrustworthy.[16]

These longstanding concerns are primed to become much more obvious and problematic as newer political uses of blockchain technologies are developed. New blockchain services are emerging that perform overt political actions, such as state, community, and private e-voting; issuing identity "documents;" management and disbursement of welfare and state benefits; smart "internet of things" public utilities management; taxation control and verification, and so on. A significant worry is that these services that have traditionally been provided by democratic states are, in strict accordance with the laws of neoliberalism, primed to be downloaded into private or pseudo-private blockchains.

12.2 Open Secrets

Blockchain technologies also enable a potentially emancipatory third way between the binaries of total secrecy and radical transparency. One of the central political challenges facing digital life today is the availability or perceived non-availability of privacy. While this topic has been studied *extensively* with respect to cryptography, usually to the end that cryptography is an effective Privacy Enhancing Technology (PET), it is not always the case that cryptography necessarily leads total or absolute privacy, or that total and absolute privacy is an obvious societal good. The possibility for an "open secret," which I propose here, is only secret in its form and so lies in open view, and therefore offers a more nuanced kind of sociality of visibility, and with it, improved political forms. Indeed, with blockchain technologies, the real secret is that there is no secret beyond the appearance. In this regard, we can see ways in which the sense of "open secret" enabled by blockchain technologies is an extension of the written letter, as for example, used by the Beat poets for their political ends.

[15] DuPont, "The Politics of Cryptography: Bitcoin and the Ordering Machines."
[16] Lustig and Nardi, "Algorithmic Authority."

In "How to be alone," Jonathan Franzen discusses the issue of privacy (as it existed in the late 1990s), and argues that we are enveloped in a "privacy panic." A privacy panic is the widespread belief that what we want, and need, more than anything, is some completely free zone or sphere of life. This view was a popular extension of liberal ideology, and dominated most discussions of privacy when Franzen wrote his essay. Little has changed, in this regard, since we seem to still be in a privacy panic, with zealots and dogmatists occupying the fashionable parts of news coverage and academic scholarship. To ask for "balance" of discourse on privacy or an assessment of competing interests is tantamount to being a political hawk. In fact, I have experienced the backlash of privacy panic myself—in an opinion article published in the *Christian Science Monitor*, I argued for the need to change discourse on privacy—this I believed was a moderate and sensible position. Because of the privacy panic, however, I was attacked by Electronic Frontier Foundation "attorneys" who argued that any mention of the word "balance" was tacit advocacy for widespread, unchecked government surveillance, and a dismantling of liberal democracy. I ended up feeling like my "moderate" argument was, unbeknownst to me, radical right-wing politics.

To make his point, Franzen critiques Richard Powers' belief that privacy amounts to "the part of life that goes unregistered." Franzen believes that the "four pages" of "recordable transactions" from a month of credit card purchases are not cause for privacy concern, let alone panic. Indeed, even when many parts of life are "registered," the intelligence gained, Franzen believes, is minimal, and not especially problematic. While I believe Franzen's diagnostic is correct, that we are in a "privacy panic," his critique of Powers' desire to go unregistered is simply outmoded—a view from a simpler time. Franzen sees no worry about the surveillance of "recordable purchases" because, when he was writing his essay, one could in good conscience think that the intelligence gained from these databases was unable to gain access to what anybody was "thinking, seeing, saying, wishing, planning, dreaming, and feeling ashamed of." This is no longer true. Today, consumer and intelligence agency databases routinely capture and derive such facts from seemingly innocent purchase histories, and from, increasingly, geographical information, online writing, viewing habits, and so on.

As I have been arguing, many people believe that encryption is our last stand against such an intrusion into the fabled sphere of privacy. I think ubiquitous cryptography, in fact, has the potential to produce the opposite effect. Encrypted communications typically have the *appearance* of protecting privacy,

and therefore *encourage* the use of these digital and online services, since, if the concerns of a privacy panic are technologically allayed, full and unthinking participation is the rational action. The result is that participation in an increasingly "recordable" life ends up filling databases with intelligence "signals," which then get used to derive what people are "thinking, seeing, saying, wishing, planning, dreaming, and feeling ashamed of," through the use of big data and sophisticated analysis. By participating, even in encrypted settings, it may be true that no *human being* can view personal and private data, but it is not necessarily true that *machines* cannot still read this data. Google's Gmail product, for example, was an early example of a large website using mandatory encryption for transmission across the open Internet. But, consequently Google relies on the fact that email content can be machine-parsed to serve ads. Outside of such closed networks, machines can invariably read plaintext metadata, from packets routing data and other sources,[17] which is invaluable for drawing insights using network analysis. Moreover, machines can often read the data itself, if the cryptographic keys are stored on the server (as is the case with many cloud storage services), or, increasingly, by using sophisticated cryptographic and data science techniques, such as using homomorphic encryption (which permits a machine to make calculations on encrypted data, without ever decrypting it), or varieties of "differential privacy" (which injects special kinds of noise to obscure *personally* identifiable data, but permits broad intelligence gathering). The end result of participating in a world of ubiquitous cryptography, in a sophisticated landscape of analysis and technological circumventions, is that the aspects of privacy that we hold dear, Franzen's "thinking, seeing, saying, wishing, planning, dreaming, and feeling ashamed of," are still available to companies, intelligence organizations, and anyone who controls the digital plumbing.

Despite the challenges that arise from the increasing use of cryptography, and the tacit recognition that technological fixes are unlikely to lead to any real balance, I want to end with one way that technology may be of assistance. To illustrate this possibility, I return to the blockchain, but drawn on the much older systems of expression. Specifically, letter writing in the mid twentieth century.

For Beat poets, the letter represented two key possibilities in Post War America: a technology of self-expression and communication opposed to the superficiality of modern mass media; and an economy of interpersonal

[17] DuPont and Fidler, "Edge Cryptography and the Co-Development of Computer Networks and Cybersecurity."

intimacy.[18] That is, the epistolary practices of Beat poets amounted to a political project of "open secrecy," as Ginsberg called it. Similar to the social environment today, the Beat poets encountered a Cold War paranoia that demanded the conscription of private selves in the name of national security. At this time everyday life was, especially for Beat poets, highly restrictive and therefore required technologies of circumvention and resistance, which the poets found in letter writing. Faced with widespread surveillance and censorship, the Beat poets did not retreat into silence but instead turned the very mechanisms of restriction into their weapons.

The Beat Poets wrote letters with full knowledge that they were going to be intercepted and read. Indeed, viewed from the outside, the letter ostensibly promised a completely secret place, but the Beat poets knew that in fact it did not. Thus, they used their knowledge of surveillance to counter it: viewed from the inside, an open secret turns known surveillance into a strategy of resistance. The correspondences between poets were destined for intelligence organizations as much as for their addressed recipients. In fact, on several occasions members were arrested based on information found in intercepted letters, which were then read back to them as an interrogation tactic. But ultimately, and here lies the real political practice, the Beat poets knew that their letters were destined for public consumption, in the many archives and anthologies that contain them today.

The Beat poets thus resisted the equal and opposite reaction that characterizes our contemporary discourse networks: the willful restriction of selves through the use of strong and ubiquitous cryptography. Rather than discoursing openly, or even weaponizing communication tools as the Beat poets once did, today we silence ourselves by hiding behind encrypted messages. But in fact this rarely works politically or pragmatically, because, like the addressed letters mailed by the Beat poets, encrypted HTTPS packets include cleartext header information that is routinely captured for traffic analysis. Perhaps, if we were to establish networks of open secrecy instead, from the outside the letter and the packet would be open to interception and censorship. But from the inside, the open secret would make the message "visible," and thus the material and political effect would be very different from today's ubiquitous cryptography.

What exactly would an "open secret" on a blockchain look like? Nothing like the highly efficient blockchains of banking and finance, which are characterized by movement and speed, and not the strongly encrypted flows of HTTPS packets either. Instead, blockchains permit the registration of norms and

[18] Harris, *William Burroughs and the Secret of Fascination*, 58.

values—as the blocks and transactions of the Merkle tree—which could conceivably replace the previous systems of secret communications and shadowy conspiring that accepts (in fact, enacts) political and personal silence. Not only does an open secret permit greater vacillation between insider and outsider, object and subject, agent and response, it shuts down the possibility of surveillance through its very transparency. Moreover, the use of technologies to establish open secrets also helps break down polarized political rhetoric, since a new, regulated but permissive space is opened up when an architecture of open secrecy is used. Although this approach does nothing to turn back the clock on ubiquitous cryptography, we might figure that, rather than fight it, we join it. Like the Beat epistolary project, the blockchain could be used to "declassify the secrets of the human body and soul,"[19] enacting new kinds of visibility and sociality.

[19] Ibid.

APPENDIX A.

Glossary

Algorithm: The deterministic process of rule following. All [encryption] steps must be algorithmic, so as to be reversible (in [decryption]).

Asymmetrical cryptography: Another term for [public key cryptography]. Refers to the fact that public key cryptography requires two linked, but distinct (asymmetrical) [keys].

Cipher: Another name for [encryption], which is also used in its noun form to refer to specific encryption [algorithms] (e.g., the "Twofish cipher").

Ciphertext: The ([ordered]) result of [encryption]. Is usually considered [secret], and suitable for [transmission] or storage.

Cryptanalysis: The process of turning [ciphertext] back into [plaintext], without access to knowledge of the [encryption] process (or the associated [key]). Distinct from the deterministic process of [decryption], cryptanalysis is fundamentally a "guess" or probability of the likelihood that the result of cryptanalysis is actually the plaintext.

Cryptogram: Or "cryptograph." Another name for [ciphertext], possibly coined by E.A. Poe. More commonly refers to non-industrial applications of cryptography, as evidenced by the name of the hobby organization, American Cryptogram Association.

Cryptography: My preferred term for the topic of this dissertation, here divided into three parts ([plaintext], [encryption], [ciphertext]). Cryptography is a complex phenomena that shifts in composition and use across history, but is essentially [notational] symbols that are activated through encryption, to produce ciphertext. Usually (but not always), cryptography refers to a process of establishing and maintaining [secrecy].

Cryptology: A top-level category that refers to the study of [cryptography] and [cryptanalysis]. It is a relatively modern term, although often used anachronistically in histories.

Decryption: The reverse process of [encryption]. Like encryption, decryption is [algorithmic] and thus ontologically and methodologically distinct from [cryptanalysis].

Encrypt: The verbal form of the noun "[encryption]."

Encryption: The active process of turning [plaintext] into [ciphertext]. Encryption must be [algorithmic], so as to avoid collapsing into a form of destruction.

Hash: An application of [encryption] that produces [ciphertext] of a predetermined length (a "hash digest"). The result is often called a "fingerprint," since each unique input produces a unique output (which can be avoided by adding another unique piece of information, called a "salt"). A distinction is sometimes made between "cryptographically-secure" hashes and those that are less robust.

Key: The [secret] information in a reusable (industrial) [encryption] process; often thought to be essential to [cryptography], but the key only becomes critical in complex "autokey" forms of cryptography (invented by Cardano) that incorporate [plaintext] in the encryption process. In modern cryptography the key is often used to initialize a pseudorandom generator, rather than by incorporating plaintext data.

Mimesis: A theory of representation that focuses on imitation, illusion, resemblance, veracity, or realism. First popularized by Plato and Aristotle, it has been widely deployed in various media studies fields, especially by those interested in "screen studies."

Notation: A system of writing that, according to Goodman's criteria, is any mark that has the properties of syntactic "disjointedness" and "finite differentiation." All [plaintext] is notational. If additional semantic criteria are added, the resulting "notational system" establishes a link between sets of marks, as in [encryption].

Order: A complex phenomena that, according to Lorand, may mean an ordering principle, or the condition of a given set (its conformity to the ordering principle). [Ciphertext] is a set of marks that have been highly ordered to look like chaos or noise.

Plaintext: An appropriately-prepared symbolic representation used as input for [encryption], typically, alphabetic writing. Must be [notational].

Public key cryptography: Invented in the 1970s, public key [cryptography] was a modern revolution in the field due to its ability to establish information [security] without first sharing a [key] between sender and receiver. The critical insight of public key cryptography is that two mathematically linked keys can be used for complex multi-pass [encryption] schemes

(such as the Diffie-Hellman key exchange). Also (originally) called "non-secret" encryption, however, one key must always remain secret (called the "private" key), while the other key (the "public" key) can be openly distributed. "Public key infrastructure" (PKI) refers to the large-scale control and management of public keys (and their associated private key pairs).

Secrecy: Fundamentally a social process, "true" secrecy, where no other parties are informed, would be a tautology and thus useless. The fundamental challenge of secrecy, then, is to share and control access to information. But by its very nature a secret is self-defeating, since any disclosure (a necessity for any non-tautological meaning) compromises the secrecy.

Security: Closely aligned with [secrecy], but may include other aspects important to modern computer and information engineering, such as confidentiality or authentication.

Symmetrical cryptography: An anachronistic term for [cryptography], sometimes called "classical" cryptography to distinguish it from [asymmetrical] or [public key cryptography].

Transmission: Typically used as a synonym to communication, I use it as a term of art in a media context, inherited from Regis Debray, who differentiates between communication across distance and transmission across time.

Bibliography

Agamben, Giorgio. *The Signature of All Things: On Method*. Translated by Luca D'Isanto and Kevin Attell. New York : Cambridge, Mass: Zone Books, 2009.

———. *"What Is an Apparatus?" and Other Essays*. 1st ed. Stanford, CA: Stanford University Press, 2009.

Agre, Philip. *Computation and Human Experience*. Learning in Doing. New York: Cambridge University Press, 1997.

Alberti, Giovanni Battista. "De Componendis Cifris." In *The Mathematical Works of Leon Battista Alberti*, edited by Kim Williams, Lionel March, and Stephen R. Wassell, 169–87. Basel: Springer Basel, 2010. http://link.springer.com.myaccess.library.utoronto.ca/content/pdf/10.1007%2F978-3-0346-0474-1_4.

"Algorithm, N." *OED Online*. Oxford University Press, December 2014. http://www.oed.com.myaccess.library.utoronto.ca/view/Entry/4959.

Al-Kadi, Ibrahim A. "Origins of Cryptology: The Arab Contributions." *Cryptologia* 16, no. 2 (1992): 97–126. doi:10.1080/0161-11929186680l.

Ambriola, V., L. Bendix, and P. Ciancarini. "The Evolution of Configuration Management and Version Control." *Software Engineering Journal* 5, no. 6 (1990): 303–10.

Anonymous. "Letter from Programmer (Item #D6) (Transcription)." *The Agrippa Files*, March 28, 1992. http://agrippa.english.ucsb.edu/letter-from-programmer-item-d6-transcription.

Assange, Julian, Jacob Appelbaum, Andy Müller-Maguhn, and Jérémie Zimmermann. *Cypherpunks*. New York: OR Books, 2012.

Austrian, G.D. *Herman Hollerith: Forgotten Giant of Information Processing*. New York: Columbia University Press, 1982.

Back, Adam. "Hash Cash Postage Implementation." *Cypherpunks*, March 28, 1997. http://www.hashcash.org/papers/announce.txt.

Bacon, Francis. *Novum Organum Scientiarum*. Venetiis: Typis G. Girardi, 1762.

———. *Of the Advancement and Proficiencie of Learning; Or, The Partitions of Sciences, Nine Books. Written in Latin by the Most Eminent, Illustrious and Famous Lord Bacon. Interpreted by Gilbert Wats.* Translated by Gilbert Wats. Golden Ball in Osier Lane, London: Thomas Wiliams, 1674. https://archive.org/details/ofadvancementproobaco.

———. "The Advancement of Learning." In *The Major Works*, translated by Brian Vickers, 120–299. Oxford World's Classics. New York: Oxford University Press, 2008.

———. *The Two Bookes of Sr. Francis Bacon. Of the Proficience and Aduancement of Learning, Divine and Hvmane*. London, Printed [by N. Okes] for W. Washington, 1629. http://archive.org/details/twobookesofsrfraoobaco.

———. "Translation of the 'De Augmentis.'" In *The Works of Francis Bacon*, edited by James Spedding, Roberts L. Ellis, and Douglas D. Heath. Boston: Houghton, Mifflin and Company, 1900. https://archive.org/details/worksoffrancisba001bacoiala.

Barlow, John Perry. "Letter from John Perry Barlow to Kevin Begos (Item #D45) (Transcription)," June 11, 1992. http://agrippa.english.ucsb.edu/letter-from-john-perry-barlow-to-kevin-begos-11-june-1992-itemd45-transcription.

Beaulieu, Yvan. "Peirce's Contribution to American Cryptography." *Transactions of the Charles S. Peirce Society* 44, no. 2 (April 1, 2008): 263–87.

Beniger, James R. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, MA: Harvard University Press, 1986.

Berkowitz, Alan, and Daniel J. Cook. "Leibniz-Bouvet Correspondence." Accessed January 19, 2016. http://leibniz-bouvet.org/.

Berry, David M. *The Philosophy of Software: Code and Mediation in the Digital Age*. Basingstoke, Hampshire; New York: Palgrave Macmillan, 2011.

Biggs, N. L. "The Roots of Combinatorics." *Historia Mathematica* 6, no. 2 (1979): 109–36.

Blanchette, Jean-François. *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*. MIT Press, 2012.

Blaze, Matt. "Protocol Failure in the Escrowed Encryption Standard." In *Proceedings of the 2Nd ACM Conference on Computer and Communications Security*, 59–67. CCS '94. New York, NY, USA: ACM, 1994. doi:10.1145/191177.191193.

Bono, James J. *The Word of God and the Languages of Man: Interpreting Nature in Early Modern Science and Medicine*. Vol. 1. 2 vols. Madison: University of Wisconsin Press, 1995.

Bowker, Geoffrey C., and Susan Leigh Star. *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: MIT Press, 1999.

Boyne, Roy. "Angels in the Archive: Lines into the Future in the Work of Jacques Derrida and Michel Serres." *Journal for Cultural Research* 2, no. 2–3 (1998): 206–222.

Bradley, Arthur. *Derrida's Of Grammatology: An Edinburgh Philosophical Guide*. Edinburgh: Edinburgh University Press, 2008. http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=243590.

Brann, Noel L. *Trithemius and Magical Theology: A Chapter in the Controversy Over Occult Studies in Early Modern Europe*. SUNY Series in Western Esoteric Traditions. Albany: State University of New York Press, 1999.

Brunton, Finn, and Helen Nissenbaum. *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press, 2015.

Buonafalce, Augusto. "Bellaso's Reciprocal Ciphers." *Cryptologia* 30, no. 1 (2006): 39–51. doi:10.1080/01611190500383581.

Cage, John. *Silence: Lectures and Writings*. Middletown, Conn.: Wesleyan University Press, 1961. http://archive.org/details/silencelectureswi961cage.

Campbell-Kelly, Martin. "Punched-Card Machinery." In *Computing Before Computers*. Ames: Iowa State University Press, 1990.

Capurro, Rafael. "Angeletics: A Message Theory." Karlsruhe, Germany, 2003. http://www.capurro.de/angeletics_zkm.html.

———. "What Is Angeletics?" Accessed August 14, 2015. http://www.capurro.de/angeletics.html.

Capurro, Rafael, and John Holgate, eds. *Messages and Messengers - Von Boten und Botschaften*. München: Fink Wilhelm GmbH + Co.KG, 2011.

Carpo, Mario. *Architecture in the Age of Printing: Orality, Writing, Typography, and Printed Images in the History of Architectural Theory*. Cambridge, MA: MIT Press, 2001.

———. *The Alphabet and the Algorithm*. Cambridge, MA: MIT Press, 2011.

Carson, Anne. *Nay Rather*. Sylph Editions. London: Center for Writers & Translators, American University of Paris, 2013.

Castells, M. *The Rise of the Network Society*. 1st ed. Vol. 1. 3 vols. Oxford, MA: Blackwell Publishing, 1996.

Cayley, John. "The Code Is Not the Text (Unless It Is the Text)." *Electronic Book Review*, September 10, 2002. http://www.electronicbookreview.com/thread/electropoetics/literal.

Chaum, David. "Blind Signatures for Untraceable Payments." edited by R.L. Rivest, David Chaum, and A.T. Sherman, 199–203. Plenum, 1982. http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF.

Cheney-Lippold, John. "A New Algorithmic Identity." *Theory, Culture & Society* 28, no. 6 (November 1, 2011): 164–81. doi:10.1177/0263276411424420.

Cherry, E. "A History of the Theory of Information." *Information Theory, IEEE Transactions on* 1, no. 1 (February 1953): 22–43.

Child, Paul W. "Cipher against Ciphers: Jonathan Swift's Latino-Anglicus Satire of Medicine." *Cryptologia* 35, no. 3 (2011): 257–66. doi:10.1080/01611194.2011.558608.

Chun, Wendy H.K. *Programmed Visions: Software and Memory*. Cambridge, MA: MIT Press, 2011.

Chun, Wendy H.K., and T. Keenan, eds. *New Media, Old Media: A History and Theory Reader*. Routledge, 2006.

Cohen, Jonathan. "On the Project of a Universal Character." *Mind*, New Series, 63, no. 249 (January 1, 1954): 49–63.

Cooke, Miriam. "Ibn Khaldun and Language: From Linguistic Habit to Philological Craft." *Journal of Asian and African Studies* 18, no. 3–4 (January 1, 1983): 179–88.

Cortada, James W. *Before the Computer: IBM, NCR, Burroughs, and Remington Rand and the Industry They Created, 1865-1956*. Princeton, NJ: Princeton University Press, 1993.

Cramer, Florian. *Words Made Flesh: Code, Culture, Imagination*. Rotterdam: Piet Zwart Institute, 2005. http://cramer.pleintekst.nl/00-recent/words_made_flesh/html/words_made_flesh.html.

Dai, Wei. "PipeNet 1.1 and B-Money." *Cypherpunks*, November 26, 1998. http://marc.info/?l=cypherpunks&m=95279516022393&w=2.

Daintith, John, and Edmund Wright, eds. "Code." *A Dictionary of Computing*. Oxford University Press, 2014. http://www.oxfordreference.com.myaccess.library.utoronto.ca/view/10.1093/acref/9780199234004.001.0001/acref-9780199234004-e-817.

Daston, Lorraine. "Marvelous Facts and Miraculous Evidence in Early Modern Europe." In *Wonders, Marvels, and Monsters in Early Modern Culture*,

edited by Peter G. Platt, 76–104. Newark: University of Delaware Press, 2000.

———. "Preternatural Philosophy." In *Biographies of Scientific Objects*, edited by Lorraine Daston, 15–41. Chicago: University of Chicago Press, 2000.

Dauenhauer, Bernard P. *Silence, the Phenomenon and Its Ontological Significance*. Studies in Phenomenology and Existential Philosophy. Bloomington: Indiana University Press, 1980.

David, Ephraim. "Sparta's Kosmos of Silence." In *Sparta: New Perspectives*, edited by Stephen. Hodkinson and Anton. Powell, 116–27. London: Duckworth with the Classical Press of Wales, 1999.

Davies, H. Neville. "Bishop Godwin's 'Lunatique Language.'" *Journal of the Warburg and Courtauld Institutes* 30 (January 1, 1967): 296–316. doi:10.2307/750747.

Davis, Martin. *The Universal Computer the Road from Leibniz to Turing*. Boca Raton, FL: CRC Press, 2012. http://public.eblib.com/choice/publicfullrecord.aspx?p=830247.

Debray, Régis. *Transmitting Culture*. Translated by Eric Rauth. European Perspectives: A Series in Social Thought and Cultural Criticism. New York: Columbia University Press, 2004.

DeCook, Travis. "Francis Bacon's 'Jewish Dreams': The Specter of the Millennium in New Atlantis." *Studies in Philology* 110, no. 1 (2013): 115–31. doi:10.1353/sip.2013.0002.

Deibert, Ronald. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Expanded edition. Toronto, ON: Signal, 2013.

Deleuze, Gilles. "Kant, Synthesis and Time." March 14, 1978.

———. "Postscript on the Societies of Control." *October* 59, no. Winter (1992): 3–7.

DeNardis, Laura. "The Internet Design Tension between Surveillance and Security." *IEEE Annals of the History of Computing* 37, no. 2 (April 2015): 72–83. doi:10.1109/MAHC.2015.29.

Derrida, Jacques. "FORS." Translated by Barbara Johnson. *The Georgia Review* 31, no. 1 (April 1, 1977): 64–116. doi:10.2307/41397444.

———. *Of Grammatology*. Translated by Gayatri Chakravorty Spivak. Corrected. Baltimore; London: The Johns Hopkins University Press, 1998.

Diffie, Whitfield, and Martin E. Hellman. "New Directions in Cryptography." *IEEE Transactions on Information Theory* 22, no. 6 (1976): 644–54.

Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Updated and expanded ed. Cambridge, Mass: MIT Press, 2007.

———. "The Export of Cryptography in the 20th and the 21st Centuries." In *The History of Information Security: A Comprehensive Handbook*, edited by Karl Maria Michael de Leeuw and Jan Bergstra, 1st ed. Amsterdam: Elsevier Science, 2007.

Diffie, Whitfield, James A. Reeds, and J. V. Field. *Breaking Teleprinter Ciphers at Bletchley Park: An Edition of I.J. Good, D. Michie and G. Timms: General Report on Tunny with Emphasis on Statistical Methods (1945)*. John Wiley & Sons, 2015.

Doyle, Sir Arthur Conan. "Silver Blaze." In *Delphi Complete Works of Sir Arthur Conan Doyle (Illustrated)*. Hastings, East Sussex: Delphi Classics, 2013.

DuPont, Quinn. "Cracking the Agrippa Code," 2012. http://www.crackingagrippa.net/.

———. "Cracking the Agrippa Code: Creativity Without Destruction." *Scholarly and Research Communication* 4, no. 13 (2013): 1–8.

———. "The Printing Press and Cryptography: Alberti and the Dawn of a Notational Epoch." In *A Material History of Medieval and Early Modern*

Ciphers: Cryptography and the History of Literacy. Edited by Katherine Ellison and Susan Kim. Material Readings in Early Modern Culture. New York, NY: Routledge, 2017.

———. "Opinion: It's Time to Rethink Polarizing Encryption Debate." *Christian Science Monitor*, December 2, 2015. http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1202/Opinion-It-s-time-to-rethink-polarizing-encryption-debate.

———. "Opinion: Why Apple Isn't Acting in the Public's Interest." *Christian Science Monitor*, February 22, 2016. http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0222/Opinion-Why-Apple-isn-t-acting-in-the-public-s-interest.

———. "Otherness and Order." In *Andrés Ramírez Gaviria: A Line, However Short, Has An Infinite Number Of Points*. Bacelona: Triton, 2016.

———. "The Politics of Cryptography: Bitcoin and the Ordering Machines." *The Journal of Peer Production* 1, no. 4 (2014). http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines.

DuPont, Quinn, and Bradley Fidler. "Edge Cryptography and the Co-Development of Computer Networks and Cybersecurity." *IEEE Annals of the History of Computing* 38, no. 4 (Oct.–Dec. 2016).

DuPont, Quinn, and Bill Maurer. "Ledgers and Law in the Blockchain." *King's Review*, June 23, 2015. http://kingsreview.co.uk/magazine/blog/2015/06/23/ledgers-and-law-in-the-blockchain/.

DuPont, Quinn, and Yuri Takhteyev. "Ordering Space: Alternative Views of ICT and Geography." *First Monday* 21, no. 8 (July 23, 2016). http://firstmonday.org/ojs/index.php/fm/article/view/6724.

Dyson, George. *Turing's Cathedral: The Origins of the Digital Universe*. New York: Vintage, 2012.

Eco, Umberto. *Semiotics and the Philosophy of Language*. Advances in Semiotics Series. Bloomington, Indiana: Indiana University Press, 1986.

———. *The Search for the Perfect Language*. Translated by James Fentress. Cambridge, Mass., USA: Blackwell, 1995.

Edgerton, David. *The Shock of the Old: Technology and Global History Since 1900*. New York: Oxford University Press, 2011.

Eisenstein, Elizabeth L. *The Printing Press as an Agent of Change*. Cambridge: Cambridge University Press, 1980. http://ebooks.cambridge.org/ref/id/CBO9781107049963.

Electronic Frontier Foundation. "Let's Encrypt." Accessed July 1, 2015. https://letsencrypt.org/.

Ellersick, F. "A Conversation with Claude Shannon." *IEEE Communications Magazine* 22, no. 5 (1984): 123–26.

Ellis, J. H. "The History of Non-Secret Encryption." *Cryptologia* 23, no. 3 (1999): 267–73. doi:10.1080/0161-119991887919.

Ellison, Katherine. "'114400072777607680000 Wayes': Early Modern Cryptography as Fashionable Reading." *Journal of the Northern Renaissance* 6 (2014). http://www.northernrenaissance.org/114400072777607680000-wayes-early-modern-cryptography-as-fashionable-reading/.

———. "Millions of Millions of Distinct Orders: Multimodality in Seventeenth-Century Cryptography Manuals." *Book History* 14, no. 1 (2011): 1–24.

Elsam, Eric. "COINS II/ARPANET: Private Line Interface (PLI) Operations Manual." Cambridge, MA: Bolt Beranek and Newman Inc., October 1980.

Enns, Anthony. "Introduction: The Media Philosophy of Sybille Krämer." In *Medium, Messenger, Transmission: An Approach to Media Philosophy*. Amsterdam: Amsterdam University Press, 2015.

Ernst, Thomas. *Schwarzweisse Magie. Der Schlussel Zum Dritten Buch Der Steganographia Des Trithemius.* Vol. 25. Zeitschrift Für Mittlere Deutsche Literatur. Daphnis, 1996.

———. "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia." *Cryptologia* 22, no. 4 (1998): 318–41. doi:10.1080/0161-119891886957.

Ernst, Wolfgang. *Digital Memory and the Archive*. Translated by Jussi Parikka. Minneapolis, MN: University of Minnesota Press, 2013. http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=586190.

Feenberg, Andrew. *Critical Theory of Technology*. New York: Oxford University Press, 1991.

———. *Questioning Technology*. New York: Routledge, 1999.

———. *Transforming Technology: A Critical Theory Revisited*. Rev Sub edition. New York, N.Y: Oxford University Press, 2002.

Finley, Klint. "It's Time to Encrypt the Entire Internet." *Wired*. Accessed November 12, 2014. http://www.wired.com/2014/04/https/.

Finney, Hal. "RPOW - Reusable Proofs of Work." *Cypherpunks*, August 15, 2004. http://marc.info/?l=cypherpunks&m=109259877510186&w=2.

Floridi, Luciano. *The 4th Revolution: How the Infosphere Is Reshaping Human Reality*. First edition. New York: Oxford University Press, 2014.

Formigari, Lia. *Language and Experience in 17th-Century British Philosophy*. Philadelphia: John Benjamins Publishing Company, 1988.

Foucault, Michel. *Foucault Live: Collected Interviews, 1961--1984*. Edited by Sylvère Lotringer. Translated by Lysa Hochroth and John Johnston. New York, N.Y.: Semiotext, 1996.

———. *The Archaeology of Knowledge*. Translated by Alan Sheridan. New York: Harper & Row, 1969.

———. *The Order of Things: An Archaeology of the Human Sciences*. New York: Routledge, 2002.

Friedman, William F. *Military Cryptanalysis: Part I Monoalphabetic Substitution Systems*. Washington, DC: United States Government Printing Office, 1938.

———. *Military Cryptanalysis: Part II Simpler Varieties of Polyaphabetic Substitution Systems*. Washington, DC: United States Government Printing Office, 1938.

———. *Military Cryptanalysis: Part III Simpler Varieties of Aperiodic Substitution Systems*. Washington, DC: United States Government Printing Office, 1939.

———. *The Index of Coincidence and Its Applications in Cryptanalysis*. A Cryptographic Series 49. Laguna Hills, CA: Aegean Park Press, 1987.

Galloway, Alexander R. "Love in the Middle." In *Excommunication: Three Inquiries in Media and Mediation*, 25–76. TRIOS. Chicago: University of Chicago Press, 2013.

———. *Protocol: How Control Exists After Decentralization*. Cambridge, MA: MIT Press, 2004.

———. *The Interface Effect*. Cambridge UK: Polity, 2012.

———. "What Is New Media?: Ten Years after the Language of New Media." *Criticism* 53, no. 3 (2011): 377–84. doi:10.1353/crt.2011.0021.

Galloway, Alexander R., Eugene Thacker, and McKenzie Wark. *Excommunication: Three Inquiries in Media and Mediation*. Chicago: University of Chicago Press, 2013.

Gardner, Martin. *Logic Machines and Diagrams*. New York: McGraw-Hill, 1958.

Giblett, Rodney James. *Sublime Communication Technologies*. Basingstoke [England] ; New York: Palgrave Macmillan, 2008.

Glidden, Hope H. "Polygraphia and the Renaissance Sign: The Case of Trithemius." *Neophilologus* 71, no. 2 (1987): 183–95. doi:10.1007/BF00209168.

Golomb, Solomon W. "On Factoring Jevons' Number." *Cryptologia* 20, no. 3 (1996): 243–46. doi:10.1080/0161-119691884933.

Golumbia, David. "Bitcoin as Politics: Distributed Right-Wing Extremism." In *MoneyLab Reader: An Intervention in Digital Economy*, edited by Geert Lovink, Nathaniel Tkacz, and Patricia de Vries, 118–31. IMC Reader 10. Amsterdam: Institute of Network Cultures, 2015.

———. *The Cultural Logic of Computation*. Cambridge, MA: Harvard University Press, 2009.

Goodman, Nelson. *Languages of Art: An Approach to a Theory of Symbols*. Indianapolis: Hackett Publishing, 1976.

Grafton, Anthony. *Leon Battista Alberti: Master Builder of the Italian Renaissance*. Cambridge, MA: Harvard University Press, 2000.

———. *Worlds Made by Words: Scholarship and Community in the Modern West*. Cambridge, MA: Harvard University Press, 2009.

Greengrass, Mark, Michael Leslie, and Timothy Raylor, eds. *Samuel Hartlib and Universal Reformation: Studies in Intellectual Communication*. Cambridge University Press, 2002.

Grometstein, Alan A., ed. *MIT Lincoln Laboratory: Technology in Support of National Security*. Lexington, Massachusetts: MIT Lincoln Laboratory, 2011.

Guillory, John. "Genesis of the Media Concept." *Critical Inquiry* 36, no. 2 (2010): 321–62. doi:10.1086/648528.

Gutas, Dimitri. "The Study of Arabic Philosophy in the Twentieth Century: An Essay on the Historiography of Arabic Philosophy." *British Journal of Middle Eastern Studies* 29, no. 1 (May 1, 2002): 5–25.

Halliwell, Stephen. *Aristotle's Poetics*. London: Duckworth, 1998.

Han, Béatrice. *Foucault's Critical Project: Between the Transcendental and the Historical*. Translated by Edward Pile. Atopia. Stanford, CA: Stanford University Press, 2002.

Hapke, Thomas. "Wilhelm Ostwald's Combinatorics as a Link between In-Formation and Form." *Library Trends* 61, no. 2 (2012): 286–303.

Harris, Oliver. *William Burroughs and the Secret of Fascination*. SIU Press, 2006.

Harris, Roy. *The Origin of Writing*. London: Duckworth, 1986.

Harrison, Steve, and Paul Dourish. "Re-Place-Ing Space: The Roles of Place and Space in Collaborative Systems." In *Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work*, 67–76. Boston, MA: Association for Computing Machinery, 1996.

Hartley, R.V.L. "Transmission of Information." Lake Como, Italy, 1927.

Hayles, N. Katherine. *Chaos Bound: Orderly Disorder in Contemporary Literature and Science*. Ithaca, NY: Cornell University Press, 1990.

———. *Writing Machines*. Cambridge, MA: MIT Press, 2002.

Heidegger, Martin. "The Question Concerning Technology." In *Basic Writings*, Revised and Expanded., 306–41. New York: HarperCollins Publishers, 1993.

Helmont, F.M. van. *The Alphabet of Nature*. Translated by Allison Coudert and Taylor Corse. Aries Book Series, v. 3. Leiden: Brill, 2007.

Hemmendinger, D. "Two Early Interactive Computer Network Experiments." *IEEE Annals of the History of Computing* PP, no. 99 (2015): 1–1. doi:10.1109/MAHC.2015.44.

Hope, Christopher. "Spies Should Be Able to Monitor All Online Messaging, Says David Cameron," January 12, 2015, sec. Technology.

http://www.telegraph.co.uk/technology/internet-security/11340621/Spies-should-be-able-to-monitor-all-online-messaging-says-David-Cameron.html.

Hugill, Peter J. *Global Communications Since 1844: Geopolitics and Technology*. Baltimore: Johns Hopkins University Press, 1999.

Hutchins, W. John. "Machine Translation: History." *Encyclopedia of Language and Linguistics*. San Diego, CA: Elsevier Science & Technology Books, 2006.

———. "Two Precursors of Machine Translation: Artsrouni and Trojanskij." *International Journal of Translation* 16, no. 1 (2004): 11–31.

Innis, Harold Adams. *Empire & Communications*. Edited by Dave Godfrey. Illustrated ed. Victoria, BC: Press Porcépic, 1986.

"Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 5." Cambridge, MA: Bolt Beranek and Newman Inc., April 1974.

"Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 7." Cambridge, MA: Bolt Beranek and Newman Inc., October 1974.

Introna, Lucas D. "The Enframing of Code." *Theory, Culture & Society* 28, no. 6 (November 1, 2011): 113–41. doi:10.1177/0263276411418131.

"IRIS." *Theoi Greek Mythology: Exploring Mythology in Classical Literature and Art*. Accessed August 21, 2015. http://www.theoi.com/Pontios/Iris.html.

Iverson, Kenneth E. "Notation As a Tool of Thought." *Commun. ACM* 23, no. 8 (August 1980): 444–465. doi:10.1145/358896.358899.

James A. Reeds, Whitfield Diffie, and J. V. Field, eds. *Breaking Teleprinter Ciphers at Bletchley Park: An Edition of I.J. Good, D. Michie and G. Timms: General Report on Tunny with Emphasis on Statistical Methods (1945)*. Hoboken, NJ: Wiley-IEEE Press, 2015.

http://ca.wiley.com/WileyCDA/WileyTitle/productCd-0470465891.html.

Jevons, Stanley W. *The Principles of Science: A Treatise on Logic and Scientific Method*. 2 vols. London: Macmillan and Co., 1874.

Johnson, Timothy Edward. "Sketchpad III, Three Dimensional Graphical Communication with a Digital Computer." Thesis, Massachusetts Institute of Technology, 1963. http://dspace.mit.edu/handle/1721.1/11559.

Jones, Steven E. *The Emergence of the Digital Humanities*. New York: Routledge, 2014.

Kahn, David. "On the Origin of Polyalphabetic Substitution." *Isis* 71, no. 1 (1980): 122–127.

———. *The Codebreakers*. Abridged. London: Sphere Books Limited, 1977.

———. *The Codebreakers: The Story of Secret Writing*. New York: Macmillan, 1967.

Kant, Immanuel. *Critique of Pure Reason*. Edited by Paul Guyer and Allen W. Wood. 15th ed. The Cambridge Edition of the Works of Immanuel Kant. Cambridge: Cambridge University Press, 2009.

Kelly, Nataly. "Why Machines Alone Cannot Solve the World's Translation Problem." *Smartling*, January 9, 2014. https://www.smartling.com/2014/01/09/machines-solve-worlds-translation-problem/.

Kelly, Thomas. "The Myth of the Skytale." *Cryptologia* 22, no. 3 (1998): 244–60. doi:10.1080/0161-119891886902.

Kember, Sarah, and Joanna Zylinska. *Life After New Media: Mediation as a Vital Process*. Cambridge, MA: MIT Press, 2012.

King, David A. *The Ciphers of the Monks: A Forgotten Number-Notation of the Middle Ages*. Stuttgart: F. Steiner, 2001.

Kirby, Vicki. "Enumerating Language: 'The Unreasonable Effectiveness of Mathematics.'" *Configurations* 11, no. 3 (2003): 417–39. doi:10.1353/con.2004.0028.

Kirschenbaum, Matthew. *Mechanisms: New Media and the Forensic Imagination*. Cambridge, MA: MIT Press, 2008.

Kirschenbaum, Matthew, Alan Liu, and Doug Reside. "No Round Trip: Two New Primary Sources for Agrippa." *The Agrippa Files*. Accessed November 15, 2015. http://agrippa.english.ucsb.edu/kirschenbaum-matthew-g-with-doug-reside-and-alan-liu-no-round-trip-two-new-primary-sources-for-agrippa.

Kitchin, Rob, and Martin Dodge. *Code/Space: Software and Everyday Life*. Cambridge, MA: MIT Press, 2011.

Kittler, Friedrich. "Code." Edited by M. Fuller. *Software Studies: A Lexicon*. Cambridge, MA: MIT Press, 2008. Google Scholar.

———. *Discourse Networks 1800/1900*. Stanford, CA: Stanford University Press, 1990.

———. *Gramophone, Film, Typewriter*. 1st edition. Stanford, CA: Stanford University Press, 1999.

———. *Optical Media*. Translated by Anthony Enns. Cambridge, UK: Polity, 2010.

———. "Protected Mode." *Bolz, Norbert (Hg.): Computer Als Medium. M\ünchen*, 1994, 209–220.

———. "There Is No Software." *CTheory* 32 (October 18, 1995). http://www.ctheory.net/printer.aspx?id=74.

———. "Towards an Ontology of Media." *Theory, Culture & Society* 26, no. 2–3 (March 2009): 23–31. doi:10.1177/0263276409103106.

Knobloch, Eberhard. "The Mathematical Studies of G.W. Leibniz on Combinatorics." *Historia Mathematica* 1, no. 4 (1974): 409–30.

Knowlson, James. *Universal Language Schemes in England and France 1600–1800*. University of Toronto Romantic Series. Toronto: University of Toronto Press, 1975.

Koopman, Colin. "Historical Critique or Transcendental Critique in Foucault: Two Kantian Lineages." *Foucault Studies*, no. 8 (March 19, 2010): 100–121.

Krämer, Sybille. *Medium, Messenger, Transmission: An Approach to Media Philosophy*. Translated by Anthony Enns. Amsterdam: Amsterdam University Press, 2015.

———. "Messenger Angels: Can Angels Embody a Theory of the Media Avant La Lettre?" *Textus* XXI, no. 8 (2008): 221–34.

———. "The Cultural Techniques of Time Axis Manipulation: On Friedrich Kittler's Conception of Media." *Theory, Culture & Society* 23, no. 7–8 (December 1, 2006): 93–109. doi:10.1177/0263276406069885.

Krentz, Christopher. *Writing Deafness: The Hearing Line in Nineteenth-Century American Literature*. Chapel Hill, NC: The University of North Carolina Press, 2007.

Lateiner, D. "Signifying Names and Other Ominous Accidental Utterances in Classical Historiography." *Greek, Roman, and Byzantine Studies* 45, no. 1 (2005): 35–57.

Leary, Thomas (Penn). "Cryptology in the 15th and 16th Century." *Cryptologia* 20, no. 3 (1996): 223–42. doi:10.1080/0161-119691884924.

Leibniz, Gottfried Wilhelm. *Dissertatio de Arte Combinatoria*. Leipzig: Joh. Simon Fickium et Joh. Polycarp., 1666. http://www.rarebookroom.org/Control/leiart/index.html?page=7.

———. "Dissertation on the Art of Combinations." In *Philosophical Papers and Letters*, edited by Leroy E. Loemker, 73–84. The New Synthese Historical Library 2. Dordrecht: Kluwer Academic Publishers, 1989.

———. "The Monadology." In *Discourse on Metaphysics and Other Essays*, translated by Daniel Garber and Roger Ariew. Indianapolis: Hackett, 1991.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

———. *Code v2*. Basic Books, 2006.

Levy, Steven. *Crypto: Secrecy and Privacy in the New Code War*. London: Penguin, 2002.

Lewis, Rhodri. "'The Best Mnemonicall Expedient': John Beale's Art of Memory and Its Uses." *The Seventeenth Century* 20, no. 1 (Spring 2005): 113–44.

———. "The Publication of John Wilkins's Essay (1668): Some Contextual Considerations." *Notes and Records of the Royal Society* 56, no. 2 (May 22, 2002): 133–46. doi:10.1098/rsnr.2002.0174.

Liu, Alan. "Commentary by Alan Liu: Cracking the Agrippa Code: How the Disk Worked (Discoveries From the 'Cracking the Agrippa Code' Contest in 2012)." *The Agrippa Files*, June 22, 2014. http://agrippa.english.ucsb.edu/post/documents-subcategories/the-disk-and-its-code/cracking-the-agrippa-code-how-the-disk-worked.

———. *Local Transcendence: Essays on Postmodern Historicism and the Database*. Chicago: University of Chicago Press, 2008.

———. *The Laws of Cool: Knowledge Work and the Culture of Information*. Chicago: University of Chicago Press, 2004.

Liu, Alan, Paxton Hehmeyer, James Hodge, Kimberly Knight, David Roh, Elizabeth Swanstrom, and Matthew Kirschenbaum. "The Agrippa Files," 2005. http://agrippa.english.ucsb.edu/.

Llull, Ramon. *Doctor Illuminatus: A Ramón Llull Reader*. Edited by Anthony Bonner. Princeton, N.J.: Princeton University Press, 1993.

Locke, William N., and A. Donald Booth, eds. *Machine Translation of Languages*. New York: The Technology Press of The Massachusetts Institute of Technology, 1955.

Long, Pamela O. *Openness, Secrecy, Authorship: Technical Arts and the Culture of Knowledge from Antiquity to the Renaissance*. Paperbacks ed. Baltimore: Johns Hopkins University Press, 2004.

Lorand, Ruth. *Aesthetic Order: A Philosophy of Order, Beauty and Art*. Routledge Studies in Twentieth Century Philosophy. New York: Routledge, 2000.

Lord, Bob. "Enigma Decrypts." Accessed March 28, 2016. http://ilord.com/bp-decrypts.html.

Lubar, Steven. "'Do Not Fold, Spindle or Mutilate': A Cultural History of the Punch Card." *Journal of American Culture* 15, no. 4 (December 1, 1992): 43–55. doi:10.1111/j.1542-734X.1992.1504_43.x.

Luebeke, David M., and Sybil Milton. "Locating the Victim: An Overview of Census-Taking, Tabulation Technology and Persecution in Nazi Germany." *IEEE Annals of the History of Computing* 16, no. 3 (1994): 25–39.

Lustig, Caitlin, and Bonnie Nardi. "Algorithmic Authority: The Case of Bitcoin," 743–52. IEEE, 2015. doi:10.1109/HICSS.2015.95.

Lux, Jonathan E. "'Characters Reall': Francis Bacon, China and the Entanglements of Curiosity." *Renaissance Studies* 29, no. 2 (April 2015): 184–203. doi:10.1111/rest.12060.

Maat, Jaap. *Philosophical Languages in the Seventeenth Century: Dalgarno, Wilkins, Leibniz*. Dordrecht: Springer, 2004.

Mackenzie, Adrian. *Cutting Code: Software and Sociality*. Digital Formations, v. 30. New York: Peter Lang, 2006.

———. "The Problem of Computer Code: Leviathan or Common Power?" Lancaster, England: Institute for Cultural Research, Lancaster

University, March 2003. http://www.lancaster.ac.uk/staff/mackenza/papers/code-leviathan.pdf.

———. "Undecidability: The History and Time of the Universal Turing Machine." *Configurations* 4, no. 3 (1996): 359–79. doi:10.1353/con.1996.0020.

Mackenzie, Adrian, and Theo Vurdubakis. "Codes and Codings in Crisis: Signification, Performativity, and Excess." *Theory, Culture & Society* 28, no. 6 (November 1, 2011): 3–23. doi:10.1177/0263276411424761.

Manovich, Lev. *The Language of New Media*. Cambridge, MA: The MIT Press, 2001.

Marino, Mark C. "Critical Code Studies." *Electronic Book Review*, December 4, 2006. http://www.electronicbookreview.com/thread/electropoetics/codology.

Markley, Robert. *Fallen Languages: Crises of Representation in Newtonian England, 1660-1740*. Ithaca, NY: Cornell University Press, 1993.

Maurer, Bill. "Money Nutters." *Economic Sociology_the European Electronic Newsletter* 12, no. 3 (July 2011): 5–13.

Maurer, Bill, Taylor C. Nelms, and Lana Swartz. "'When Perhaps the Real Problem Is Money Itself!': The Practical Materiality of Bitcoin." *Social Semiotics* 23, no. 2 (April 2013): 261–77. doi:10.1080/10350330.2013.777594.

Mayr, Otto. *Authority, Liberty & Automatic Machinery in Early Modern Europe*. Baltimore, London: The Johns Hopkins University Press, 1986.

Meister, Aloys. *Die Geheimschrift Im Dienste Der Päpstlichen Kurie Von Ihren Anfängen Bis Zum Ende Des XVI. Jahrhunderts*. Paderborn, 1906. https://archive.org/details/diegeheimschrifoomeisgoog.

Merchant, Carolyn. "'The Violence of Impediments': Francis Bacon and the Origins of Experimentation." *Isis* 99, no. 4 (December 1, 2008): 731–60. doi:10.1086/597753.

Misa, Thomas J. *Leonardo to the Internet: Technology & Culture from the Renaissance to the Present*. Johns Hopkins Studies in the History of Technology. Baltimore: The Johns Hopkins University Press, 2004.

Mitchell, Christine. "Situation Normal, All FAHQT Up: Language, Materiality & Machine Translation." PhD, McGill University, 2010.

Morozov, Evgeny. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs, 2014.

Mosco, Vincent. *The Digital Sublime: Myth, Power, and Cyberspace*. Cambridge, MA: MIT Press, 2004.

Mrayati, Mohammed, Meer Alam Yahya, and at-Tayyan Hassan, eds. *Al-Kindi's Treatise of Cryptanalysis*. Translated by Said M. al-Asaad. The Arabic Origins of Cryptology 1. Riyadh: KFCRIS & KACST, 2003.

———. , eds. *Ibn `Adlan's Treatise Al-Mu'allaf Lil-Malik al'Asraf*. Translated by Said M. al-Asaad. The Arabic Origins of Cryptology 2. Riyadh: KFCRIS & KACST, 2005.

Naur, Peter, and Brian Randell, eds. *Software Engineering: Report on a Conference Sponsored by the Nato Science Committee, Garmish, Germany, 7th to 11th October 1968*. Brussels, Belgium: Scientific Affairs Division, NATO, 1969. http://homepages.cs.ncl.ac.uk/brian.randell/NATO/nato1968.PDF.

Naylor, David, Alessandro Finamore, Ilias Leontiadis, Yan Grunenberger, Marco Mellia, Maurizio Munafò, Konstantina Papagiannaki, and Peter Steenkiste. "The Cost of the 'S' in HTTPS," 133–40. Sydney, Australia: ACM Press, 2014. doi:10.1145/2674005.2674991.

"Network Encryption - History and Patents." Accessed August 6, 2015. http://www.toad.com/gnu/netcrypt.html.

Nissenbaum, Helen. "Privacy as Contextual Integrity." *Wash. L. Rev.* 79 (2004): 119.

Norberg, A.L. "Changing Computing: The Computing Community and DARPA." *IEEE Annals of the History of Computing* 18, no. 2 (Summer 1996): 40–53. doi:10.1109/85.489723.

Nyquist, Harry. "Certain Factors Affecting Telegraph Speed." *Bell System Technical Journal* 3, no. 2 (April 1924): 324–46.

O'Dwyer, Rachel. "The Revolution Will (Not) Be Decentralised: Blockchains." *P2P Foundation*, March 23, 2015. https://blog.p2pfoundation.net/the-revolution-will-not-be-decentralised/2015/03/23.

Ohala, John J. "Christian Gottlieb Kratzenstein: Pioneer in Speech Synthesis." Hong Kong, 2011.

Ong, Walter J. *Orality and Literacy: The Technologizing of the Word*. New Accents. New York: Routledge, 2002.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015.

Pesic, Peter. "François Viète, Father of Modern Cryptanalysis - Two New Manuscripts." *Cryptologia* 21, no. 1 (1997): 1–29. doi:10.1080/0161-119791885733.

———. *Labyrinth: A Search for the Hidden Meaning of Science*. Cambridge, Mass.: MIT Press, 2000.

———. "Secrets, Symbols, and Systems: Parallels between Cryptanalysis and Algebra, 1580-1700." *Isis* 88, no. 4 (December 1, 1997): 674–92.

———. "Wrestling with Proteus: Francis Bacon and the 'Torture' of Nature." *Isis* 90, no. 1 (March 1999): 81–94.

Peters, John Durham. "Assessing Kittler's Music Und Mathematik." In *Kittler Now: Current Perspectives in Kittler Studies*, edited by Stephen Sale and Laura Salisbury, 22–43. Theory Now. London: Polity, 2015.

Picard, Max. *The World of Silence*. Washington, DC: Gateway, 1964.

Plato. *Complete Works*. Edited by John M. Cooper and D. S. Hutchinson. Indianapolis, IN: Hackett Publishing, 1997.

Plutarch. "Lysander." In *Plutarch's Lives: IV Alcibiades and Coriolanus, Lysander and Sulla*, translated by Bernadotte Perrin, 233–322. Loeb Classical Library 305. Cambridge Mass.: Harvard University Press, 1959.

Podjarny, Guy. "HTTPS Adoption *doubled* This Year." *Snyk*, July 20, 2016. https://snyk.io/blog/https-breaking-through/.

Poe, Edgar Allan. "The Gold Bug." *Philadelphia Dollar*. June 28, 1843. http://www.fultonhistory.com/highlighter/highlight-for-xml?uri=http%3A%2F%2Fwww.fultonhistory.com%2FNewspapers%2520 23%2FPhiladelphia%2520PA%2520Dollar%2520Newspaper%2FPhiladelp hia%2520PA%2520Dollar%2520Newspaper%25201843-1846%2FPhiladelphia%2520PA%2520Dollar%2520Newspaper%25201843-1846%2520-%25200105.pdf.

———. *The Gold Bug*. London: George Routledge & Sons, Limited, 1894.

Poole, William. "Nuncius Inanimatus. Seventeenth-Century Telegraphy: The Schemes of Francis Godwin and Henry Reynolds." *The Seventeenth Century* 21, no. 1 (Spring 2006): 45–72.

Poovey, Mary. *A History of the Modern Fact: Problems of Knowledge in the Sciences of Wealth and Society*. Chicago: University of Chicago Press, 1998.

Raley, Rita. "Code.surface || Code.depth." *Dichtung Digital*, 2006. http://www.dichtung-digital.org/2006/01/Raley/index.htm.

———. "Machine Translation and Global English." *The Yale Journal of Criticism* 16, no. 2 (2003): 291–313. doi:10.1353/yale.2003.0022.

Reeds, Jim. "Solved: The Ciphers in Book III of Trithemius's Steganographia." *Cryptologia* 22, no. 4 (1998): 291–317. doi:10.1080/0161-119891886948.

Reitman, Rainey. "Snowden's Motivation: What the Internet Was Like Before It Was Being Watched, and How We Can Get There Again." *Electronic Frontier Foundation*, October 23, 2014. https://www.eff.org/deeplinks/2014/10/snowden-motivated-what-internet-was-it-was-being-watched-and-how-we-can-get-there.

Rescher, Nicholas. "Leibniz's Machina Deciphratoria: A Seventeenth-Century Proto-Enigma." *Cryptologia* 38, no. 2 (April 3, 2014): 103–15.

Roberts, Lawrence G. "Machine Perception of Three-Dimensional Solids." Thesis, Massachusetts Institute of Technology, 1963. http://dspace.mit.edu/handle/1721.1/11589.

Robertson, Adi. "Edward Snowden: 'Would I Do It Again? Absolutely Yes.'" *The Verge*, March 10, 2014. http://www.theverge.com/2014/3/10/5488348/edward-snowden-on-surveillance-encryption-and-constitution-at-sxsw.

Romberch, Johann Host von. *Congestorium Artificiose Memorie*. Uenetijs: Per Melchiorem Sessam, 1533. http://digitalcollections.nypl.org/collections/congestorium-artificiose-memorie-upf-jonis-romberch-de-kyrspe-omnium-de-memoria?filters%5Bname%5D=Host+von+Romberch,+Johann+(fl.+1485-1532)&keywords=#/?tab=about.

Rosenheim, Shawn. *The Cryptographic Imagination: Secret Writings from Edgar Allen Poe to the Internet*. Baltimore: The Johns Hopkins University Press, 1997.

Rossi, Paolo. *Logic and the Art of Memory: The Quest for a Universal Language*. London: Athlone Press, 2000.

Rotman, Brian. *Mathematics as Sign: Writing, Imagining, Counting*. Stanford, Calif.: Stanford University Press, 2000.

Ruparelia, Nayan B. "The History of Version Control." *SIGSOFT Software Engineering Notes* 35, no. 1 (January 2010): 5–9. doi:10.1145/1668862.1668876.

Salmon, Vivian. "The Evolution of Dalgarno's 'Ars Signorum.'" In *Studies in Language and Literature in Honour of Marget Schlauch*, 353–71. Studies in Language and Literature. New York: Russell & Russell, 1971.

Schott, Gaspar. *Organum Mathematicum*, 1668. https://commons.wikimedia.org/wiki/File:OrganumMathematicum.jpg.

Schulz, Thomas. "Translate This: Google's Quest to End the Language Barrier." *Spiegel Online*, September 13, 2013, sec. International. http://www.spiegel.de/international/europe/google-translate-has-ambitious-goals-for-machine-translation-a-921646.html.

Schwartz, Kathryn A. "Charting Arabic Cryptology's Evolution." *Cryptologia* 33, no. 4 (2009): 297–304. doi:10.1080/01611190903030904.

———. "From Text to Technological Context: Medieval Arabic Cryptology's Relation to Paper, Numbers, and the Post." *Cryptologia* 38, no. 2 (April 3, 2014): 133–46.

Scott, Brett. "Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain." *E-International Relations*, June 1, 2014. http://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/.

Serres, Michel. *Angels, a Modern Myth*. Paris: Flammarion, 1995.

———. *Hermes: Literature, Science, Philosophy*. Edited by Josué V. Harari and David F. Bell. Baltimore: Johns Hopkins University Press, 1982.

Shannon, Claude. "A Mathematical Theory of Cryptography." Murray Hill, NJ: Bell Labs, September 1, 1945. http://www.cs.bell-labs.com/who/dmr/pdfs/shannoncryptshrt.pdf.

———. "Communication Theory of Secrecy Systems." *Bell System Technical Journal* 28, no. 4 (1949): 656–715.

Shannon, Claude, and Warren Weaver. "A Mathematical Theory of Communication." *Bell System Technical Journal* 27 (1948): 379–423.

Shea, William R. "Descartes and the Rosicrucian Enlightenment." In *Metaphysics and Philosophy of Science in the Seventeenth and Eighteenth Centuries: Essays in Honour of Gerd Buchdahl*, edited by Gerd Buchdahl and R. S. Woolhouse. Springer, 1988.

Shumaker, Wayne. *Renaissance Curiosa: John Dee's Conversations with Angels, Girolamo Cardano's Horoscope of Christ, Johannes Trithemius and Cryptography, George Dalgarno's Universal Language*. Medieval & Renaissance Texts & Studies 8. Binghamton, NY: Center for Medieval & Early Renaissance Studies, 1982.

Siegert, Bernhard. *Relays: Literature as an Epoch of the Postal System*. Translated by Kevin Repp. 1 edition. Stanford, CA: Stanford University Press, 1999.

———. "The Map Is the Territory." *Radical Philosophy* 169 (October 2011): 13–16.

Slaughter, Mary M. *Universal Languages and Scientific Taxonomy in the Seventeenth Century*. Cambridge: Cambridge University Press, 2010.

Slayton, Rebecca. "Measuring Risk: Computer Security Metrics, Automation, and Learning." *IEEE Annals of the History of Computing* 37, no. 2 (April 2015): 32–45. doi:10.1109/MAHC.2015.30.

Sontag, Susan. "The Aesthetics of Silence." *Aspen*, n.d. http://www.ubu.com/aspen/aspen5and6/threeEssays.html.

Steiner, George. *After Babel: Aspects of Language and Translation*. Third Edition. New York: Oxford Paperbacks, 1998.

Stolzenberg, Daniel, ed. *The Great Art of Knowing: The Baroque Encyclopedia of Athanasius Kircher*. Florence, Italy: Stanford University Libraries, 2001.

Strasser, Gerhard F. *Lingua Universalis: Kryptologie Und Theorie Der Universalsprachen Im 16. Und 17. Jahrhundert*. Vol. 38. Wolfenbütteler Forschungen. Wiesbaden: Harrassowitz, 1988.

———. "Ninth-Century Figural Poetry and Medieval Easter Tables—Possible Inspirations for the Square Tables of Trithemius and Vigenère?" *Cryptologia* 34, no. 1 (2009): 22–26. doi:10.1080/01611190903384970.

———. "The Noblest Cryptologist." *Cryptologia* 7, no. 3 (1983): 193–217. doi:10.1080/0161-118391857946.

———. "The Rise of Cryptology in the European Renaissance." In *The History of Information Security: A Comprehensive Handbook*, edited by Karl Maria Michael de Leeuw and Jan Bergstra, 1st ed., 277–325. Elsevier Science, 2007.

Sutherland, Ivan Edward. "Sketchpad: A Man-Machine Graphical Communication System." Dissertation. Cambridge, UK: Cambridge University, September 2003.

Tatlow, Ruth. *Bach and the Riddle of the Number Alphabet*. New York: Cambridge University Press, 1991.

Thomas, Douglas. "Hacking the Body: Code, Performance and Corporeality." *New Media & Society* 7, no. 5 (October 1, 2005): 647–62. doi:10.1177/1461444805056010.

Thomsen, Samuel W. "Some Evidence Concerning the Genesis of Shannon's Information Theory." *Studies in History and Philosophy of Science* 40, no. 1 (March 1, 2009): 81–91.

Thrift, Nigel, and Shaun French. "The Automatic Production of Space." *Transactions of the Institute of British Geographers* 27, no. 3 (2002): 309–335. doi:10.1111/1475-5661.00057.

"Tom McCarthy Remembers Friedrich Kittler." *LRB Blog*. Accessed April 4, 2015. http://www.lrb.co.uk/blog/2011/11/09/tom-mccarthy/kittler-and-the-sirens/.

Tritheme, M.I. *Polygraphie: Universelle Escriture Cabalistique de M.I. Tritheme Abbé*. Paris: Jaques Keruer, 1561. http://fantastic.library.cornell.edu/bookrecord.php?record=F034.

Trithemius, Johannes. *Steganographia (Secret Writing)*. Edited by Joseph H. Peterson, 1999. http://www.esotericarchives.com/tritheim/stegano3.htm.

Trobsky, Ian. *Black MIDI*, February 27, 2016. https://commons.wikimedia.org/wiki/File:Blackmidi.png.

Uckelman, Sara L. "Computing with Concepts, Computing with Numbers: Llull, Leibniz, and Boole." In *Programs, Proofs, Processes*, edited by Fernando Ferreira, Benedikt Löwe, Elvira Mayordomo, and Luís Mendes Gomes, 427–37. Lecture Notes in Computer Science 6158. Springer Berlin Heidelberg, 2010. http://link.springer.com/chapter/10.1007/978-3-642-13962-8_47.

Vickers, Brian. "Francis Bacon, Feminist Historiography, and the Dominion of Nature." *Journal of the History of Ideas* 69, no. 1 (2008): 117–41. doi:10.1353/jhi.2008.0007.

Vickers, Brian., ed. *Occult and Scientific Mentalities in the Renaissance*. New York: Cambridge University Press, 1984. http://myaccess.library.utoronto.ca/login?url=http://dx.doi.org/10.1017/CBO9780511572999.

Virilio, Paul. *Speed and Politics*. 2006 ed. Semiotext(e) Foreign Agents Series. Los Angeles, CA: Semiotext(e), 2006.

Wark, McKenzie. "A Slow Reader's Books of the Year." *Public Seminar*, January 10, 2016. http://www.publicseminar.org/2016/01/readings2015/.

———. "The Weird Global Media Event and the Tactical Intellectual [Version 3.0]." In *New Media, Old Media: A History and Theory Reader*, edited by Wendy H.K. Chun and T. Keenan. Routledge, 2006.

Weaver, Warren. "Recent Contributions to the Mathematical Theory of Communication." *The Mathematical Theory of Communication*, 1949, 93–117.

———. "Translation." In *Machine Translation of Languages*, edited by William Nash Locke and Andrew Donald Booth. Technology Press of Massachusetts Institute of Technology, 1955.

West, Stephanie. "Archilochus' Message-Stick." *The Classical Quarterly*, New Series, 38, no. 1 (January 1, 1988): 42–48.

Whitney, Elspeth. "Paradise Restored. The Mechanical Arts from Antiquity through the Thirteenth Century." *Transactions of the American Philosophical Society*, New Series, 80, no. 1 (1990): 1–169.

Wiedijk, Freek. "Original Text of Gibson's 'Agrippa' Poem Extracted From Disk," July 17, 2011. http://agrippa.english.ucsb.edu/post/documents-subcategories/the-disk-and-its-code/original-text-of-gibsons-agrippa-poem-extracted-from-disk.

Wigner, Eugene P. "The Unreasonable Effectiveness of Mathematics in the Natural Sciences." *Communications on Pure and Applied Mathematics* 13, no. 1 (1960): 1–14.

Wilding, Nick. "'If You Have A Secret, Either Keep It, Or Reveal It': Cryptography and Universal Language." In *The Great Art of Knowing: The Baroque Encyclopedia of Athanasius Kircher*, edited by Daniel Stolzenberg, 93–103. Firenze, Italia: CADMO, 2001.

Wilkins, John. *Essay Towards a Real Character and a Philosophical Language*. London: Royal Society, 1668.

———. *Mercury: Or, The Secret and Swift Messenger. Shewing, How a Man May with Privacy and Speed Communicate His Thoughts to a Friend at Any Distance.* 1st ed. Fleetstreet, neer Saint Dunstans Church, London: I. Norton, 1641.

———. *Mercury: Or, The Secret and Swift Messenger. Shewing, How a Man May with Privacy and Speed Communicate His Thoughts to a Friend at Any Distance. Reprinted from the Third Edition (1708)*. Foundations of Semiotics 6. Amsterdam; Philadelphia: John Benjamins Publishing Company, 1984.

Williams, Kim, Lionel March, and Stephen R. Wassell, eds. *The Mathematical Works of Leon Battista Alberti*. Basel: Springer Basel, 2010. http://link.springer.com.myaccess.library.utoronto.ca/content/pdf/10.1007%2F978-3-0346-0474-1_4.

Winthrop-Young, Geoffrey. *Kittler and the Media*. Cambridge, UK: Polity Press, 2011.

Wolfram, Stephan. "Mathematical Notation: Past and Future." In *MathML and Math on the Web*. Urbana-Champaign, IL, 2000. http://www.stephenwolfram.com/publications/mathematical-notation-past-future/.

Wright, Aaron, and Primavera De Filippi. "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," 2015. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

Yates, Frances Amelia. *The Art of Memory*. London: Routledge & Kegan Paul, 1966.

Yates, J. "Early Interactions Between the Life Insurance and Computer Industries: The Prudential's Edmund C. Berkeley." *IEEE Annals of the History of Computing* 19, no. 3 (July 1997): 60–73.

Ycart, Bernard. "Alberti's Letter Counts." *Literary and Linguistic Computing* 29, no. 2 (June 1, 2014): 255–65. doi:10.1093/llc/fqt034.

———. "Letter Counting: A Stem Cell for Cryptology, Quantitative Linguistics, and Statistics." *Historiographia Linguistica* 40, no. 3 (2013): 303–30. doi:10.1075/hl.40.3.01yca.

Yost, Jeffrey R. "The Origin and Early History of the Computer Security Software Products Industry." *IEEE Annals of the History of Computing* 37, no. 2 (April 2015): 46–58. doi:10.1109/MAHC.2015.21.

Young, James O. *Art and Knowledge*. New York: Routledge, 2001.

Zielinski, Siegfried. *Deep Time of the Media: Toward an Archaeology of Hearing and Seeing by Technical Means*. Translated by Gloria Custance. The MIT Press, 2008.

Zimmerman, Philip. "Why I Wrote PGP," 1999. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

Zook, Matthew, and Mark Graham. "From Cyberspace to DigiPlace: Visibility in an Age of Information and Mobility." *Societies and Cities in the Age of Instant Access*, 2007, 241–254.