Data Encryption Standard

In 1972, the NBS Institute for Computer Sciences and Technology (ICST) initiated a project in computer security, a subject then in its infancy. One of the first goals of the project was to develop a cryptographic algorithm standard that could be used to protect sensitive and valuable data during transmission and in storage. Prior to this NBS initiative, encryption had been largely the concern of military and intelligence organizations. The encryption algorithms, i.e., the formulas or rules used to encipher information, that were being used by national military organizations were closely held secrets. There was little commercial or academic expertise in encryption. One of the criteria for an acceptable encryption algorithm standard was that the security provided by the algorithm must depend only on the secrecy of the key, since all the technical specifications of the algorithm itself would be made public. NBS was the first to embark on developing a standard encryption algorithm that could satisfy a broad range of commercial and unclassified government requirements in information security.

Ruth M. Davis, then Director of ICST, asked the National Security Agency (NSA) to help evaluate the security of any cryptographic algorithm that would be proposed as a Federal standard. She then initiated the standard's development project by publishing an invitation in the *Federal Register* (May 15, 1973) to submit candidate encryption algorithms to protect sensitive, unclassified data. NBS received many responses demonstrating interest in the project, but did not receive any algorithms that met the established criteria. NBS issued a second solicitation in the *Federal Register (*August 17, 1974) and received an algorithm from the IBM Corp., which had developed a family of cryptographic algorithms, primarily for financial applications. After significant review within the government, NBS published the technical specifications of the proposed algorithm in the *Federal Register* (March 17, 1975), requesting comments on the technical aspects of the proposed standard. NBS received many comments on the security and utility of the proposed standard and held two public workshops during 1976 on its mathematical foundation and its utility in various computer and network architectures. After intense analysis of the recommendations resulting from the workshops, NBS issued the *Data Encryption Standard* (DES) as Federal Information Processing Standard (FIPS) 46 on November 23, 1977 [1].

Many NBS, NSA, and IBM technical staff members participated in this initiative, which combined expertise from government and industry. In 1973 the Bureau hired Dennis Branstad to lead the new computer security project and to coordinate the DES development process. Miles Smid joined NBS in 1977 to aid in the adoption of the DES in numerous American National Standards. Both worked with their former NSA colleagues to ensure that the standard met its technical criteria and was useful in many commercial and government applications. The major IBM contributors to the design of the DES algorithm and its subsequent adoption as a Federal standard included: Horst Feistel, inventor of a family of encryption algorithms of which DES is a member; Alan Konheim and Don Coppersmith, mathematicians in the IBM research organization; Walter Tuchman, director of the IBM cryptographic competency center and the primary designer of the final DES algorithm; and Carl Meyer and Mike Matyas, who worked with Tuchman in specifying the DES and analyzing its security.

DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study. . . . Today, DES is still the primary algorithm used to protect data in the financial services industry.

After NBS published the DES, the algorithm was adopted as an ANSI standard [2] in 1981 and incorporated in a family of related standards for security in the financial services industry. The DES became the world's most widely used encryption algorithm, particularly to protect financial information. Today, the American financial services industry depends almost entirely on the DES to encrypt financial transactions.

The DES algorithm is a block cipher that uses the same binary key both to encrypt and decrypt data blocks, and thus is called a symmetric key cipher. DES operates on 64-bit "plaintext" data blocks, processing them under the control of a 56-bit key to produce 64 bits of encrypted ciphertext. Similarly, the DES decryption process operates on a 64-bit ciphertext block using the same 56-bit key to produce the original 64-bit plaintext block.

DES uses a sequence of operations, including several substitution and permutation primitives, to encrypt a data block. These primitives are subsequently used to reverse the encryption operation. Horst Feistel defined a variety of substitution and permutation primitives which are iteratively applied to data blocks for a specified number of times [3,4]. Each set of primitive operations is called a "round," and the DES algorithm uses 16 rounds to ensure that the data are adequately scrambled to meet the security goals. The secret key is used to control the operation of the DES algorithm. Each key contains 56 bits of information, selected by each user to make the results of the encryption operations secret to that user. Any of approximately 10^{16} keys could be used by the DES, and an attacker trying to "crack" a DES encrypted message by "key exhaustion" (trying every key) must, on average, try half of the total possible keys before succeeding.

The development of the DES was not without controversy. There were two main objections:

1. NSA worked with NBS throughout the DES development, evaluated the proposed DES algorithm, and recommended several changes to IBM. Specifically, IBM made changes to the S-boxes, the nonlinear substitution transformations that are the heart of the algorithm, to improve the security of the DES. During one of the public workshops, Tuchman stated that he had changed the S-boxes to satisfy a security requirement that he had not previously known, and that his group had optimized S-box operations to satisfy a technical constraint of the electronics that they were currently using. Some critics suspected that NSA had deliberately weakened, rather than strengthened, the S-boxes, or perhaps even introduced a "trap door" that would enable the intelligence part of the agency to decrypt messages encrypted by the DES.

2. A commonly accepted definition of a good symmetric key algorithm, such as the DES, is that there exists no attack better than key exhaustion to read an encrypted message. Critics argued that the 56-bit DES key was too short for long-term security, and that expected increases in computer power would soon make a 56-bit key vulnerable to attack by exhaustion [5]. NBS responded that the standard was adequate against any practical attack for the anticipated life of the standard and would be reviewed for adequacy every five years. Moreover, although NBS did not stress this in their public response, NBS and Tuchman knew that the "DES core" could be used three times on the same block of data to extend the effective key length to 112 or 168 bits. The critics were not satisfied, contending that encrypted data would remain sensitive for more than 5 years and that DES would be very hard to change once it became widely used.

In retrospect, the DES has proved to be much better than initially thought by its critics. After a quarter century, the DES has proved remarkably resistant to cryptanalytic attack, including attacks unknown in the open literature in the 1970s. It seems certain that, as Touchman stated, the S-box changes did strengthen the DES in order to withstand several attacks that were not public in 1977.

However, the critics were correct about the continuing improvement in electronic technology. While the lifetime of the DES standard was originally estimated to be 15 years, it is still a Federal Information Processing standard 23 years later. Due to the improvements in technology, any 56-bit secret-key algorithm such as the DES is now vulnerable to key exhaustion using massive, parallel computations. In 1997, a message encrypted with the DES was "cracked" in about 5 months by key exhaustion using a large network of computers. In 1998, the Electronic Freedom Foundation (EFF) constructed a special purpose electronic device to decrypt messages encrypted by the DES using custom-built semiconductor chips at a cost of about $130,000 [6]. The EFF "DES Cracker" can find the key used by the DES to encrypt a message in an average of about 4.5 days, and using more chips could reduce this time.

The current Data Encryption Standard (FIPS 46-3) [7] recommends an iterative use of the original DES algorithm (as the DES development team envisioned in the 1970s) known as "Triple DES" or "DES-3." DES-3 encrypts each block three times with the DES algorithm, using either two or three different 56-bit keys. This approach yields effective key lengths of 112 or 168 bits. DES-3 is considered a very strong algorithm, and one recent paper [8] suggests that a 112-bit symmetric key algorithm such as DES-3 should be secure until about the year 2050. The original 56-bit DES algorithm is widely used to protect financial transactions today and can easily be modified to be interoperable with DES-3 and a 112-bit key. Some cryptographers regard DES-3 as the most conservative

choice for very long-term data protection, since the core DES algorithm has been so thoroughly analyzed.

NIST not only made a significant contribution in technology through its development of the DES, but also gained valuable experience in developing such important, but potentially controversial, standards. In 1997, Miles Smid, then manager of the Security Technology Group, initiated the Advanced Encryption Standard (AES) development project. The anticipated AES, is intended to be the DES successor and, like the DES, will be a symmetric key block encryption algorithm. The AES will offer larger key sizes (up to 256 bits) than the DES. However, since DES-3 appears to be secure for some time in the future, the primary near term advantage of the AES is that it will be designed for software implementation and be much faster than DES-3 on most platforms. Barring some unforeseen breakthrough in cryptanalysis or computing power, the AES should be secure for many decades. In response to a public solicitation by NIST, interested parties submitted 21 candidate algorithms to be considered for adoption as the AES. Of those submitted, fifteen met NIST's initial criteria for consideration and five very good algorithms were selected in August 1999 for additional analysis and review. NIST expects to announce the final selection in 2001. NIST, having gained increased stature within the security technology community through its experience gained by its DES initiative, is able to conduct the selection process in an open manner that virtually precludes suspicion of secret trap doors.

Dennis Branstad, who shepherded the development of the original DES, received his Ph.D. in Computer Science from Iowa State University, and worked at the National Security Agency before coming to NBS in 1973. Denny is widely respected in the cryptographic community for his technical abilities, his sage judgment and his considerable interpersonal skills. He has been a mentor and friend to many in the Computer Security Division. At the time of his retirement in 1994, Denny was a NIST Fellow.

Miles Smid received his BS in mathematics from the Univ. of Chicago and his MA in mathematics from the Univ. of Maryland. Miles came to NBS from the National Security Agency in 1977 and worked on the development of numerous Federal Information Processing Standards and ANSI standards in cryptography. Miles was the manager of the NIST Security Technology Group through most of the 1990s, a difficult period of contentious, highly charged policy as well as technical issues in cryptography. Nevertheless, he managed to be respected by nearly everyone, whatever their policy views, as both a cryptographer and a "straight shooter." Miles orchestrated the still ongoing AES effort in a manner that seems to have satisfied a very broad range of often-contentious interests and which promises to result in a very broadly accepted and used standard. Miles was Acting Chief of the Computer Security Division at the time of his retirement in 1999.

The DES can be said to have "jump started" the nonmilitary study and development of encryption algorithms. In the 1970s there were very few cryptographers, except for those in military or intelligence organizations, and little academic study of cryptography. There are now many active academic cryptologists, mathematics departments with strong programs in cryptography, and commercial information security companies and consultants. A generation of cryptanalysts has cut its teeth analyzing (that is trying to "crack") the DES algorithm. In the words of cryptographer Bruce Schneier [9], "DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study." An astonishing share of the open literature in cryptography in the 1970s and 1980s dealt with the DES, and the DES is the standard against which every symmetric key algorithm since has been compared.

One of the consequences of this development of nonmilitary cryptography has been validation of the basic model of public specification and review of encryption algorithms that NBS pioneered with the DES. The DES is well trusted because it has been so intensely studied, but the past 20 years are replete with examples of algorithms designed in secret, whose users attempted to keep the algorithm secret. In many of these cases, not only was the algorithm exposed by reverse engineering or by leaks, but the algorithm, or the overall cryptographic system that used it, was also shown to be insecure after it was already in wide use in products such as digital cellphones or digital video disk players. In addition, many software products offer ad hoc, homebrew encryption which has been cracked by experts after only a few days of study, and there are commercially available products that decrypt files protected by such programs. Time has shown that the public approach NBS chose for developing the DES standard was the best approach from a security point of view. Security by obscurity does not work.

In summary, the DES was a pioneering and farsighted standard which helped set a new paradigm for openly published and reviewed encryption standards. The DES has been an enormously useful and influential standard and remains, when used in its Triple DES mode, secure today, a quarter century after it was first proposed. It is

also, today, still the primary algorithm used to protect data in the financial services industry. The new AES standard builds on the legacy of DES and should meet our needs well into the new century.

Prepared by William E. Burr.

Bibliography

[1] *Data Encryption Standard,* Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC (1977).

[2] *Data Encryption Algorithm (DEA),* ANSI X3.92-1981, American National Standards Institute, New York.

[3] Horst Feistel, Cryptography and Computer Privacy, *Sci. Am.* **228** (5), 15-23 (1973).

[4] Horst Feistel, *Block Cypher Cryptographic System,* US Patent 3,798,359, March 19, 1974.

[5] Whitfield Diffie and Martin E. Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, *Computer* **10** (6), 74-84 (1977).

[6] Electronic Frontier Foundation, *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design,* O'Reilly & Associates, Inc., Sebastopol, CA (1998).

[7] *Data Encryption Standard (DES),* Federal Information Processing Standards Publication (FIPS PUB) 46-3, National Institute of Standards and Technology, Gaithersburg, MD (1999).

[8] Arjen K. Lenstra and Eric R. Verheul, Selecting Cryptographic Key Sizes (http://www.cryptosavvy.com/) October 1999.

[9] Bruce Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code in C, Second edition,* John Wiley and Sons, New York (1996) p. 267.