The Islamic University of Gaza
Deanery of Graduate Studies
Faculty of Engineering
Computer Engineering Department

Master Thesis

DATA ENCRYPTION USING THE DYNAMIC LOCATION AND SPEED OF MOBILE PHONE

تشفير البيانات بالاعتماد على ديناميكية المكان و سرعة الهاتف النقال

Souhir M. Elkourd

Supervisor

Prof. Hatem M. Hamad

A Thesis Submitted in partial fulfillment of the Requirements for the degree of
Master of Science in Computer Engineering

Gaza, Palestine

(1431, 2010)

Abstract

The development of applications and services of mobile phone has created a phenomenon of spying and deception through these mobiles. So, it is necessary to think of finding solutions to overcome this problem. In this thesis, we propose a new method to protect data sent between mobile phones. This method depends on one of the available services to mobile phones, such as Global Position System (GPS), Wireless Fidelity (Wi-Fi) ,.., by using the coordinate that are read through these services.

A mobile receiver with this location service registers a set of coordinates and velocity during movement and using the algorithm to estimates the next position after fixed time. Our proposed algorithm is to generate the secret key which uses this new coordinate and the dynamic tolerance distance (DTD) to increase its practicality.

The security analysis in our practical implementation shows that the probability to break this key is almost impossible due to the dynamic coordinates and (DTD) and adjusting the length of the Random key. Our proposed solution is tested in real time using (J2ME) software where the experimental study shows that the cipher text (message) can only be decrypted under the restriction interval of (DTD).

Our simulation illustrates that the proposed algorithm is more effective, practical, and promising for data transmission in mobile environment compared with existing solutions.

الملخص

إن تطوير الخدمات و التطبيقات في الأجهزة النقالة سمح بانتشار ظاهرة التجسس و الخداع على هذه الأجهزة. وعليه كان من الضروري التفكير في إيجاد حلول لهذه المشكلة.

في هذه الأطروحة تم اقتراح طريقة جديدة لحماية البيانات المرسلة من خلال هذه الأجهزة. هذه الطريقة تعتمد على خدمة متوفرة في الجهاز الجوال مثل (GPS,WI-FI،...) حيث يتم استخدام الإحداثيات التي يتم قراءتها من خلال هذه الخدمة.

الجهاز المستقبل يجب أن يحتوي على خدمة تحديد المكان حيث يقوم بتسجيل مجموعة من الإحداثيات و السرعة أثناء الحركة ويقوم البرنامج المقترح بتوقع الإحداثية التالية التي من المفترض أن يصل إليها بعد زمن ثابت.

البرنامج المقترح يقوم بإنشاء المفتاح السري حيث يعتمد على الإحداثية الجديدة المتوقعة و المسافة المسموح بها (DTD) للزيادة في دقة التطبيق.

الدراسة التحليلية في الجانب العملي بينت أن احتمال كسر هذا المفتاح هو شبه مستحيل نظرا لديناميكية الإحداثيات و DTD بالإضافة الى التعديل في المفتاح عشوائي.

هذا الاقتراح تم فحصه في الواقع باستخدام برنامج المحاكاة (J2ME) حيث أن النتائج بينت أن النص آو الرسالة المشفرة لا يتم فكه إلا في مجال DTD . ومن الواضح أن هذا البرنامج المقترح هو أكثر فعالية وعملية لحماية البيانات المتنقلة في بيئة المحمول مقارنة مع الحلول القائمة حاليا.

Résumé

Le développement d'applications et de services de téléphones mobiles, a créé un phénomène d'espionnage et de déceptions par ces mobiles. Donc, il est nécessaire de penser à trouver des solutions à ce problème. Dans cet article, nous proposons une nouvelle méthode pour protéger les données transmises entre les téléphones mobiles. Mon approche repose sur l'un des services offerts (GPS, WIFI, ..) en utilisant les coordonnées. Un récepteur mobile avec service de localisation enregistrer un ensemble de coordonnées et la vitesse pendant le mouvement et d'estimer la position suivante. Notre algorithme est de générer la clé secrète qui utilise cette nouvelle coordonnée et la distance de tolérance dynamique (DTD) pour augmenter sa pratique. L'analyse de la sécurité dans la mise en œuvre pratique montre que la probabilité de casser cette clé est presque impossible en raison de la dynamique des coordonnées et DTD et en ajustant la longueur de la clé aléatoire. Ma solution est testée en temps réel en utilisant un logiciel j2me où l'étude expérimentale montre que le texte chiffré ne peut être déchiffré en vertu de l'intervalle de restriction de la DTD. Il illustre le fait que notre algorithme est plus efficace et pratique pour la transmission de données dans un environnement mobile par rapport aux solutions existantes.

Acknowledgment

First of all I’m very thankful to my Allah who gave me the strength to carry out this study.

Special thanks to my supervisor Prof. Hatem Hamad for his aid and guide through my work in this project. I would also like to offer my gratitude to him for his accurate observations which has rich ideas.

Many thanks to my teachers, the professors: Hatem Hamad, Ibrahim abuhaiba, Mohammed Mikki and Dr. Wissam Ashour for their valuable information they have provided to us during the phase of the study.

I would also like to thank all my colleagues specially my best friends Maaly Awad, Hanan Abuthuraya and Huda Hubboub for their encouragement.

Finally, I express my grateful appreciation to my parents for their encouragement and support to complete this thesis. Deep gratitude goes to my brothers and sisters in particular my brother youcef who always help me materially and morally.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption System
API	Application Programming Interface
CDC	Connected Device Configuration
CLDC	Connected Limited Device Configuration
DES	Data Encryption Standard
DoS	Denial of Service
DTD	Dynamic Toleration Distance
ECC	Elliptic Curve Cryptography
E-OTD	Enhanced Observed Time Difference
GIF	Graphics Interchange Format
GPS	Global Positioning System
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communications
ID	Identification
IP	Internet protocol
RC	Relay Chat
JPEG	Joint Photographic Experts Group.
JVM	Virtual Machine
J2EE	Java 2 Enterprise Edition
J2ME	Java (2), Java Platform, Micro Edition
J2SE	Java 2 Standard Edition

MD5	Message-Digest algorithm 5
MIDI	Musical Instrument Digital Interface
MIDP	Mobile Information Device Profile
MMS	Multimedia Messaging Service
MP3	Media Player 3
MPEG	Moving Picture Experts Group
NIST	National Institute of Standards and Technology
OS	Operating System
P2P	Peer-to-Peer
PDA	Personal Digital Assistant
PVT	Position, Velocity and Time
RC5	Rivest's Code 5
RFID	Radio Frequency Identification
RMS	Record Management System
SHA	Secure Hash Algorithm
SMS	Short Messaging Service
TDT	Tolerance distance
TOA	Time of Arrival
VM	Virtual Machine
Wi-Fi	Wireless Fidelity

INTRODUCTION

Overview: In wireless communication, the security is a fundamental priority where the system and the data stored or transmitted/received should be protected against unauthorized access, modification, destruction or use. The security in mobile phone such as in wireless networks should have a big concern due to its wide use and sensitive information.

Today, the increasing use of mobile phone in different fields such as accessing the internet in which multiple features are available, ranging from capturing and playing digital media, to e-mail access, to e-banking also sending messages and making calls. All these applications make it easier for numbers of attack to penetrate the mobile devices. These attacks include steal information, identity, resources and spying. Moreover, they could be launched through viruses and worms by downloading software from the internet or try to attract users through the delivery of personal information such as bank account and other confidential information.

As a result, it is needed to think about solutions to develop secure mobile phone services and information. There are many ways of security provided by most of the organizations which have a sufficient handle on the majority of the threats such as firewalls, isolating the internal network resources from many attacks that are circulating in the internet or by other techniques [15]. All of these solutions provide adequate protection. However, they are not sufficient to protect the information in the devices or through transmission such as Short Message Service (SMS) and Multimedia Message Service (MMS). This area represents a new challenge, and can be an important tool in dealing with specific types of security threats.

The most important powerful and basic solution for the security threats is the cryptography which is an important tool for security where any leakage in data has become ever greater concern. So any violations will affect the public confidence in the products and services.

The encryption is an important tool used to address specific security threats, and will become increasingly important with the growth of mobile phone technology especially in the area of encrypting data. This is because of many possible attacks that threat the process of data exchange between the sender and the receiver. By the encryption of such data during transmission or reception, the confidentiality of sensitive data in transmission is protected.

Cryptographic mechanisms are a suitable means to reduce or to eliminate the above mentioned risks and to enhance the security of open distributed systems.

The history of cryptography begins thousands of years ago. When, Julius Caesar adopted the primitive idea to encrypt the messages directed to the army which based on replacing each letter by 3rd letter [40,51,11,54].

For example, the phrase: "meet me after the toga party" is encrypted to

"PHHW PH DIWHU WKH WRJD SDUWB"

Eight centuries later, the Arab civilization has developed the athletes' scientists and Arab linguists of this science in which the cryptography are used. The most famous scientists are Canadian Faraaheedi and Commas who develop advanced mathematical concepts such as compatibility and exchange [52].

In the nineteenth century, the cryptography appears useful in warfare and security for the country and people. World War I was one of the first wars that used cryptography to its fullest potential. It was also continued into World War II and used in even more conniving ways [40].

Until recent decades, it has been using a classic cryptography. These methods of encryption use simple mechanical aids like a pen and paper. Early in the 20th century, the invention of complex methods provides more sophisticated and efficient means of encryption unsuited to pen and paper [11].

In this study, we aim to protect the data sent between mobile phones where spying and spoofing have become a major threat to confidential data, especially in financial transactions as well as in military terms.

Data security in mobile phones became more realistic to users which have become a source of concern because of the radio signals and the limited memory and computing power for most mobile phone allows wireless systems vulnerable to a serious data theft, which makes thinking to provide security solutions from attacks. New dynamic location is applied in our secret key to integrate leading security solutions in the key encryption/decryption.

So, anyone who is new to security field may ask the following questions in which we try to answer in the next chapters throughout this thesis.

What is the security?

What is the hacking technique in mobile phone?

What is the security technique?

What is the cryptography?

How can we protect these mobile devices?

- Report Organization

This thesis is organized as follow: In chapter the theory of the security fundamental basics in mobile phone is presented. Then, in chapter 2, present related work where a brief overview is given about the existing previous works. After that, in chapter 3 describe our proposed algorithm which includes the generation protocol of our secret key. In chapter 4, the study of J2ME software and our practical implementation and result are provided. Finally, concluding remarks and future work are makes in chapter 5.

Chapter 1

Fundamental Study in Security

This chapter presents the theoretical overview in security, attack, and the cryptography which is used as a solution in our study. It is meant to be an introduction to get an impression of the complete system that is going to be used in the following chapters.

1.1 Security Definition

Security is the protection of the system and the data stored there in against unauthorized access, modification, destruction or use [61].

In mobile phone communication, the security is the fundamental importance where the system should be secured against brute force attacks and impersonation by the eavesdropper [25.p1].

The security takes three forms; physical security, virtual security, and data security [12].

- **Physical Security** is the protection of the physical assets, such as access points, wired channels, and the ultimate nodes [12].

- **Virtual Security** is the ability to keep data secure when access is possible without physical access, such as access over a network [12].

- **Data Security** is generally the purpose and result of physical and virtual security, e.g., to deny an unauthorized persons access to data in transit or storage [12].

1.2 Overview

With the increasing use of mobile phone technologies and mobile internet services, the number of attacks is increased to penetrate the mobile devices to steal information, identity and resources. Data leakage has become ever greater concern. Any violations will affect the public confidence in the products and services. So, it is necessary to think about methods to help in developing secure mobile phone services and information.

There are several types of attacks that can be exposed to mobile devices in terms of eavesdropping or attack on the data during transmission or reception.

1.3 Hacking Techniques in Wireless Networks

Today, data security in mobile devices becomes more realistic to users and it has become a source of concern because of the radio signals [35]. The limited memory computing power, especially accessing the internet for most mobile phones, have left wireless systems vulnerable to a serious data theft and powerful distributed computing. Such vulnerabilities, when being exploited by the hacker, can motivate the development of a variety of hacking techniques. These hacking techniques directly lead to cyber attacks and these cyber attacks have become more and more serious threat to the society [39].

1.3.1 Mobile Phone Attack

There are several techniques for the attack [39] [10] [53], among them as follow:

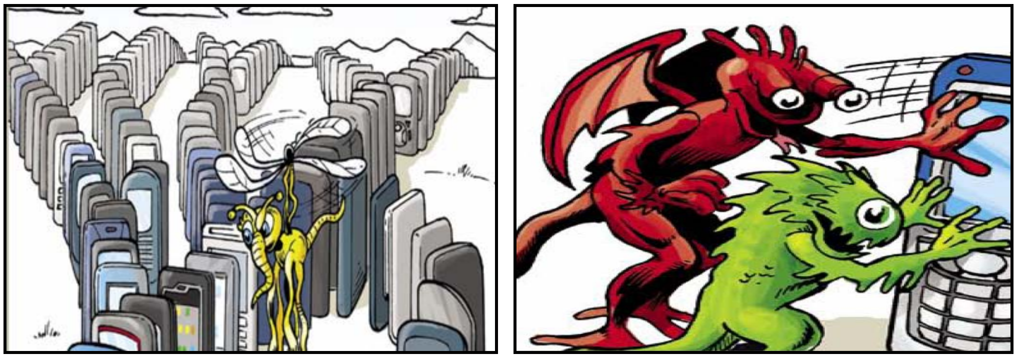


Figure 1-1: Malware mobile [50]

- Bluetooth Technique:

Most devices today have included Bluetooth services which used in several cases. For examples, in hands-free headsets for mobile phones, wireless keyboards, wireless mice, wireless printers, and wireless game controllers [13]. This allows many of the attackers, easily to break through the devices via Bluetooth technology when the devices are available to receive or send data between them which is done by sending a signal that allows the two devices to be connected. This allows an attacker to detect this signal and could also attempt to pair with one device and hack in to steal their Personal

Identification Number (PIN). And therefore, they could seize all the data stored in the device in many ways such as [13]:

- Stealing information stored on the device, including contact lists, e-mail, and text messages.
- Sending unsolicited text messages or images to other Bluetooth-enabled devices.
- Accessing the mobile phone commands, which allows the attacker to use this phone to make phone calls, send text messages, read and write phonebook contacts, eavesdrop on conversations, and connect to the internet.

- **Virus Technique:** Is malicious software that can copy itself to files or create files that may be executed in some way or sent to users as an email attachment and infect a device.

- **Worm Technique:** Is a small program independent from other programs. It has manufactured to carry out destructive or in order to steal some data from some users while surfing the internet, or cause damage or callers their own, characterized by rapid proliferation and difficult to get rid of them because of their high zigzags and reincarnation and the shuffle. An example of worm is Tanatos which is a famous worm that surfaced during the month of October 2002 [15].

- **Trojan Technique:** A program that is usually given away for free and has a hidden purpose. It may be some type of file such as a video that user's may be interested in. The user would normally install and run this program although the installation would be so simple and user would be unaware of it. This program may or may not use a vulnerability to spread. Trojan horse programs are not like viruses and worms, but it is a program could be free downloaded by e-mail attachments infected or by using the web browser when a user visits a site web. The main functions of the Trojan horse programs are to prevent data, modify, delete and disable the operation of computers or computer networks. In addition it can also include receiving and sending when installing them and restarting the infected computer and often used as intruders "clusters" consisting of Trojan horse programs is integrated.

- **Hacker Technique**: Is a programmer who breaks into computer systems deliberately without the knowledge of the owner in order to steal, change, or destroy information by exploiting device software vulnerabilities on the victim's mobile.

- **Spyware Technique:** Is software of the type malware that is installed on devices which obtains information from user's device without the user's knowledge or his consent. This technique is not serious as the rest of the techniques mentioned earlier, but many free programs contain spyware such as the current popular free zip program. The risk lies when it hides itself from the user to prevent it from being removed.

- **Backdoor Technique:** A program allows an unauthorized user remote access to infect devices which are a sub-category of backdoor Trojans which often use Internet Relay Chat (IRC) or Peer-to-Peer (P2P) protocols as their main method of communications.

So, this makes thinking to provide security solutions from attacks, by developing secure mobile phone services which enhances the security of data processing and transferring. The information security factors are confidentiality, integrity and availability [53,35,14,30,10].

1.4 Security Objectives

Information security is to protect the information resources whether it is in the devices or through messaging or voice call.

1.4.1 Confidentiality: Is the most common aspect of information security. It prevents the disclosure of information to unauthorized individuals or systems which protect the confidentiality of the information that keeps data secret from both inside and outside eavesdroppers. This is essential in financial transactions and wars. Confidentiality of data is dealing with the problems of spoofing and traffic analyses [14,53].

- **Snooping:** This refers to unauthorized access through objection the data of the victim [53].

- **Traffic Analysis:** This refers to the techniques of intercepting and examining messages by monitoring online traffic in order to deduce information from encrypted messages [53].

Confidentiality is necessary but it is not sufficient for protecting personal information.

1.4.2 Integrity: Which guarantees the protection against unauthorized modification or destruction of information where the change in data forgery or tampered with in an unauthorized way. Integrity of data is dealing with the following problems [14,53]:

- **Modification:** Is the change and interception of the message by the attacker [53].

- **Masquerading:** Or spoofing is the personating of somebody else by the attacker [53].

- Replaying: Occurs when attacker succeeds to obtain a copy of a message sent by a user who tries to replay it later [53].

- Repudiation: Is to deny the sent message by the sender and later the receiver deny that he has received the message [53].

1.4.3 Availability: The information that need to be constantly changed where it was created and stored by users. It must be accessible to authorized entities which protected from Denial of Service attack (DoS) [14,53].

- **Denial of Service:** is an attack on a site or service in a web site's through requests or messages which makes this system unable to respond to normal requests (e.g., inability to log in to an account or access a service).

1.4.4 Authentication is to assure the source of the data and its reliability [10,30].

1.5 Mobile Devices Security and Measures

Many security issues in mobile networks are essentially the same as those described above. However, security protocols developed for desktop (PCs) do not work well on mobile devices [14]. The mobility and wireless natures of mobile networks make the security more challenging. Indeed, special design attention is needed to provide an acceptable security level for mobile devices.

Therefore, the mobile security measures are treated in three levels [14]:

1. The mobile-user level,
2. The mobile data and applications level, and
3. The network communications level.

1.5.1 Security Attacks on Mobile Devices [14.p8]

There are two modes of security attack on mobile devices [14,53]; active mode or passive mode.

In active mode the attacker makes damage in the target mobile system completely and instantly. The main methods for this mode use denial of service (DOS), man-in-the-middle, and theft. This mode of attacks is more detrimental [53,14].

In passive mode the attacker does not attempt to damage the target mobile system. It mainly harms the target by spoofing, eavesdropping, and installing malicious code [14]. The collected information can be used to analyze the target mobile system and thus steal the confidential information. This mode of attacks is more difficult to detect. [14].

1.6 Security Techniques

The actual implementation of security goals needs some techniques. Two techniques are prevalent today; cryptography and steganography [53].

In our work, the cryptography technique is applied because it is more widely used specially in wireless communications.

1.6.1 Cryptography Techniques is the science of writing or reading coded messages, encompassing the principles and methods of transforming an intelligible message into one that is unintelligible then retransforming that message back to its original form [11,53].

1.6.2 Steganographic Techniques means striving to hide the very presence of the message itself from an observer [53].

Many different carrier file formats can be used for hiding secret information. There exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information while others require larger secret message to be hidden.

Many solutions are proposed to protect mobile phone such that antivirus, firewall, SMS anti-spam, and data encryption [62,63].

Encryption is an important tool used to address specific security threats and will become increasingly important with the growth of mobile phone technology especially in the area of encryption of data sent through mobile phone such as SMS and MMS. This represents a new challenge and can be an important tool in dealing with specific types of security threats.

Cryptographic mechanisms are suitable means to reduce or to eliminate the above mentioned risks and to enhance the security of open distributed systems.

1.7 Cryptography

Cryptography is the art and science of keeping messages secured which means “secret writing.” It is derived from the two Greek words 'crypto' which means 'secret' and 'graph' which means 'writing' [11,55,56,57].

Cryptography refers almost exclusively to encryption which is the process of protecting information (plaintext or original data) by transforming it into an unreadable format (cipher-text or unintelligible data). The information is encrypted using a "key" that makes the data unreadable. It is later decrypted, making the information readable again.

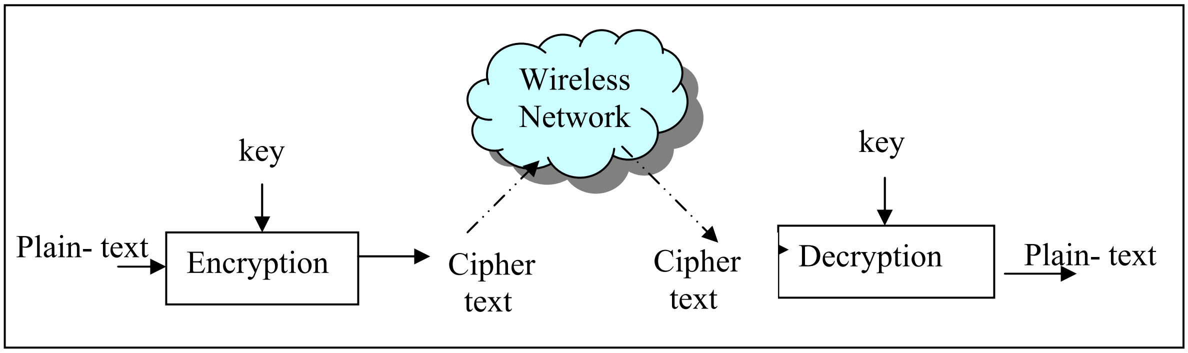


Figure 1-2: Cryptography operation

In the past, Cryptography helped ensuring secrecy in important communications such as those of spies, military leaders and diplomats [31]. However, in recent decades, cryptography has expanded its remit in two ways:

- Mechanisms for more than just keeping secrets, schemes like digital signatures and digital cash.

- In widespread use by many civilians, and users are not aware of it.

Thus, it is the basic building block that enables the mechanisms of authentication, integrity, and confidentiality.

Cryptography uses two main styles or forms of encrypting data; symmetrical and asymmetrical.

1.7.1 Symmetric Encryptions Algorithm which uses the same key for encryption as they do for decryption as in Figure 1-3. The encryption key can be loosely related to the decryption key. The key is secret and is shared by the message sender and recipient [53,60,16].

- **The Encryption Algorithm** is a process of translating a message called the plain-text into an encoded message called the cipher-text [53].

- **The Decryption Algorithm**: is the reverse process to encryption. Frequently, the same cipher is used for both encryption and decryption while encryption creates a cipher-text from a plain-text, decryption creates a plain-text from a cipher-text[53,16].

Plain-text: is an unencrypted message, before it is passed through an encryption algorithm.

Cipher-text: is encoded text after it has been passed through an encryption algorithm. It is the product of plain-text after encryption [53,16].

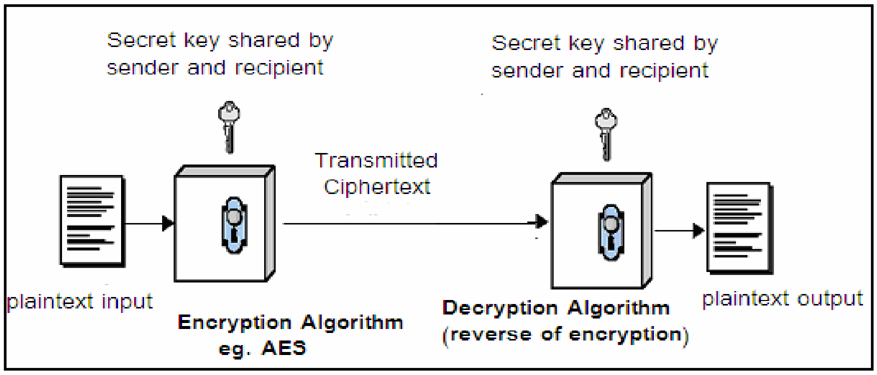


Figure 1-3: Symmetric cipher model

In addition, there exist two types of symmetric-key algorithms stream ciphers and block ciphers [53,16].

Stream Cipher: Where the message is encrypted one bit / byte at a time (Figure 1-4).

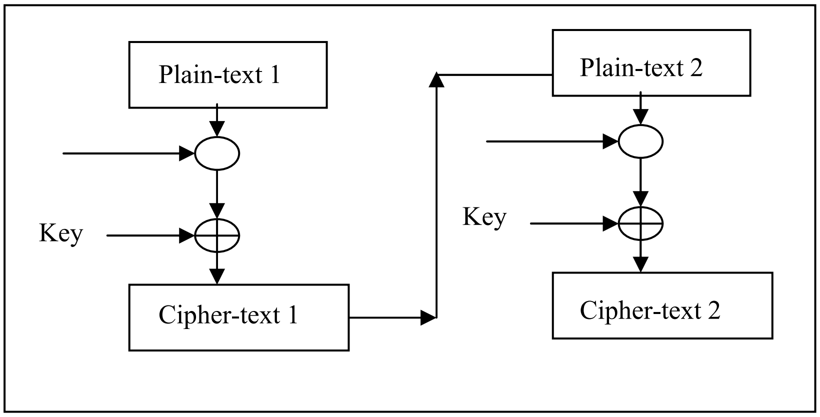


Figure 1-4: Stream cipher

Block Cipher: is one in which a block of message is treated as a whole of n used to produce a cipher-text block of equal length (Figure 1-5).

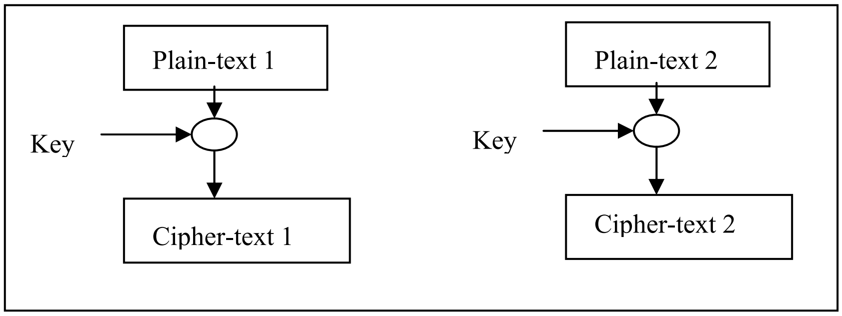


Figure 1-5: Block cipher

Some popular examples of symmetric algorithms are (AES), (RC4), (DES) and (TDES). Similarly, the decryption algorithm takes, n-bit block of cipher-text together with the secret key and yields the original n-bit block of plaintext.

The secret key used in this thesis, applying block cipher in symmetric key example of block cipher is (AES).

In general, a block cipher consists of two paired algorithms; one for encryption, (E) and the other for decryption (E^{-1}). Both algorithms accept two inputs; an input block of size n bits and a key of size (k) bits, yielding an n-bit output block. For any one fixed key, decryption is the inverse function of encryption, so that

$$E_K(M) = C\ ; \quad E_K^{-1}(C) = M$$

For any block (M) and key (K). (M) is termed the plain-text and (C) the cipher-text. Most block ciphers are constructed by repeatedly applying a simpler function. Each iteration is termed a round and the repeated function is termed the round function; anywhere within (4 to 32) rounds are typical. Usually, the round function (R) takes different round keys (K_i) as second input which is derived from the original key:

$$M_i = R_{K_i}(M_{i-1}) \text{ And } C = M_r \oplus K_{r+1}$$

(M_0) is the plain-text and (M_r) the cipher-text while (r) being the round number. In the current algorithms, (AES) symmetric encryption is used.

AES versus DES: (AES) is a relatively new algorithm compared with (DES). Observing that (DES) is more and more out of date and (3DES) is not a long term replacement candidate for the widely used (DES) algorithm. The National Institute of Standards and Technology (NIST) called a new Advanced Encryption Standard (AES). (AES) is more secured than (DES). It has key length as long as (256) bits. It also has high computation efficiency and flexibility to be practical in a wide range of applications. The security level of (AES) is (128,192,256) depending on the used key size where the (AES) block sizes are (128, 192) and (256). (NIST) defines risk management as "the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level." However, these guidelines lack a quantitative method for modeling risk in order to asses it [24].

1.7.2 Asymmetric Encryption:

The asymmetrical encryption is the approach that uses two different keys for encryption and decryption. The key used for decryption is a secret private key whereas the encryption key is a published public key [53,16]. Thus, anyone in possession of the public encryption key may encrypt and send a message to the holder of the private decryption key where the key used to encrypt a message is not the same as the key used to decrypt it. However, only the holder of the private decryption key may decipher the message. These two keys are created and used in conjunction. The essential protection in asymmetric encryption is confidentiality and integrity.

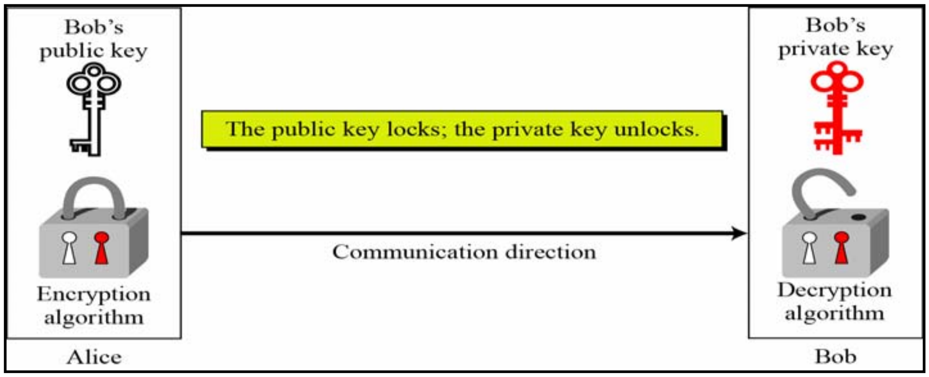


Figure 1-6: Asymmetric Encryption [22]

Encryption function C = f (K-public, P).

Decryption function P = g (K-private, C)

Where (C) is the cipher-text and (P) is the plain-text. Some popular examples of asymmetric algorithms are (RSA, ElGamal, elliptic curve, RABIN).

In the proposed secret key of this study, RSA asymmetric encryption code is applied where the receiver partner sends his dynamic information as (SMS) encrypted message to the sender. (See the details in chapter3).

The most common public-key algorithm is Rivest, Shamir, and Adleman (RSA) covers only short messages for a 1024-bit RSA key. (RSA) uses modular exponentiation for encrypt/decrypt.

$C= P^{e}$ mod n, (e, n) are public-key.

$P= C^{d}$ mod n, d is a privet-key.

(n) is a big number with a value between -2^{1023} and 2^{1024}.

Encrypted messages will be of the length (128) bytes. The maximum size of an encrypted message is (117) bytes. When sending longer messages, a hybrid system is used in which a small bunch of random bits only encrypts (128 bits) and uses that bunch as a key for a symmetric encryption system (e.g. AES). This process can handle much longer messages (and the process is much faster, too) [17].

Symmetric and asymmetric-key cryptography will exist in parallel and continue to serve the community. It is actually believed that they are complements of each other; the advantages of one can compensate for the disadvantages of the other [53].

There are several types of cryptographic mechanisms among them as follow:

Encipherment, data integrity, digital signature, authentication exchange, traffic, padding, routing control, notarization, and access control which provide the security services that is close to each other, but in different fields to detect, prevents and recovers from a security attack.

1.8 Cryptographic Hash Function:

Cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string which is called the hash value or the message digest (Figure 1-7).

In general, a cryptographic hash function (H ( )) should have the property that given an input value N, it is efficiently computable to obtain the hash value H (N). However, given H (N) is computationally difficult to get back the value N. A cryptographic hash function is insecure if [26]:

- The attacker finds a message that matches a given hash value.

- The attacker succeeds to find two different messages that have the same hash value.

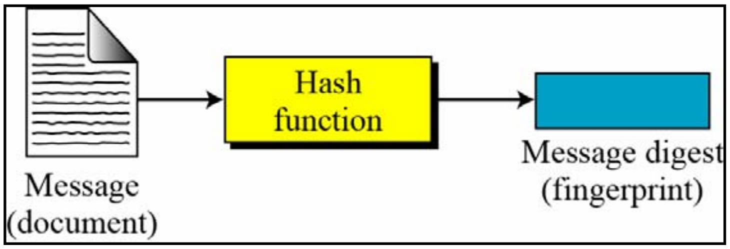


Figure 1-7: Hash function [22]

There is a long list of cryptography hash functions such as (SHA-0, SHA-1, SHA-2, SH-512, MD5) Whirlpool and so on. In our algorithm, any type of hash function can be used. This work is specified by applying the cryptography hash function (MD5) as example shown in chapter3.

The cryptography hash function (MD5) is one of the standard hash functions for a long time creates digests of (128) bits. To break this hash function, it needs to test $(2^{128/2}) = 2^{64}$ tests. Even if the adversary can perform 2^{30} (more than one billion) tests in a second, it takes 2^{34} seconds (more than 500 years) to launch an attack [18].

1.9 Multimedia Messaging Service (MMS):

Multimedia Messaging Service (MMS) is a communications technology developed by Third Generation Partnership Project (3GPP) which allows users to exchange multimedia communications from one mobile to another. It is also possible to send (MMS) messages from a mobile phone to an email address. (MMS) includes text (formatted with fonts, colors, etc), sounds (MP3, MIDI), images (JPEG, GIF format and video (MPEG) [58,59].

With the increasing use of mobile technologies, the number of attacks increases through the mutual message and mobile services that makes a big damage in personal information and financial transactions. This occurs through the growing use of internet in mobile devices. So, information and services can be saved by developing new security system which provides the confidentiality, integrity and availability.

Chapter 2
Related Work

In this chapter, some previous work related to our proposed algorithm in this thesis are discussed. Extensive researches have been done on data encryption for wireless networks and mobile phone transmission. However, few of these researches have focused on using dependant location to secure mobile devices.

For example, in [2] Hsien-Chou and Yun-Hsiang, proposed a Location Data Encryption Algorithm (LDEA). The purpose of (LDEA) is mainly to include the latitude/longitude coordinate to be used as the key for data encryption in (LDEA). The cipher-text can only be decrypted at the expected location. A Toleration Distance (TD) is designed to overcome the inaccuracy and inconsistent problem of (GPS) receiver.

The strength of the key depends only on the random key, the latitude and longitude coordinate is not strong enough. That is because they are using the static location of mobile node and they are using a static Toleration Distance (TD) to overcome the inaccuracy and inconsistence of (GPS) receiver. On the other hand, the decryption is done while the mobile is moving very slowly which gives high successful rate of decryption. But when the mobile is moving with high speed, it was very difficult to perform successful decryption and that makes the successful rate of decryption equal to zero in the case of high-speed which demonstrates why the use of this approach is limited.

In [3], Al-Fuqaha and Al-Ibrahim, proposed a (GPS- based encryption-geo encryption) protocol by restricting the decryption of a message to a particular location and time period. This protocol related in mobility model for existing geo-encryption techniques to allow mobile nodes to exchange movement parameters. However, the sender is able to geo-encrypt messages to a moving decryption zone that contains a mobile node's estimated location. However, this protocol is limited to a static location and can not be used in dynamic location.

In [4], Scott and Denning et al. proposed a location-based encryption approach by using the (GPS), called Geo-Encryption. The Geo-Encryption is to limit the area inside which the intended recipient can decrypt messages. A geo-locking function is employed during the encryption process to combine an encryption key where the data was encrypted according to the expected Position, Velocity and Time (PVT) of the receiver with the recipient's geographic location (L) to produce a "geo-secured" key for transmission alongside an encrypted message; the message can only be decrypted if the geo-secured key is recovered.

However, the (PVT-to-geo-Lock) mapping function is the primary mechanism to ensure that the data is decrypted successfully. This can only be done if the recovering device is physically positioned at location (L). The sender also transmits parameters which define the shape of the area where decryption zone is permitted and the time period duration where decryption can be accomplished. This approach is based on the traditional encryption system and communication protocol. Also, they noted that the velocity parameter for the recipient can be added to the geo-locking function. However, no details of mobility are supported in this approach.

In [5], Mundt proposed a location dependent digital rights management system which is based on a trusted hardware incorporating the decryption of digital data, a precise secure clock, and a (GPS) position receiver. This idea uses authenticated position information delivered by Galileo which enables access to restricted digital material or to be restricted devices. A secret key can only be utilized to decrypt the digital material or to enable any other process when the device is in the specified area. So, Location is essential for controlling access to resources protected by the digital rights. This method uses the dataset to specify the shape of static location where the access is permitted which makes it easy to break this secret key.

Examples of other applications to secure location are as follow:

In [6], Vijayalakshmi and Palanivelu proposed public key cryptography scheme for secure localization and authentication between sensor nodes in wireless sensor networks. Their (TOA) location based authentication scheme is built on the ID-based cryptography by using (ECC) and (ECC) key exchange. Also they compared between this technique and other asymmetric algorithms like (RSA) and (MPRSA). The exchange of the key is also done using Diffie-Hellman and then compared so as to prove that (ECC) is the best.

In [7], Liao et al. proposed a static location-dependent data encryption approach for mobile information system. The approach is based on a reverse hashing principle. A series of session keys is generated based on one-way hash function. They are generated for mobile client and server in a secure network simultaneously. When the mobile client is operated in an insecure network of the outdoor environment, the session key is incorporated with the (GPS) coordinate for ensuring that the data is decrypted at the desired location.

In [8], Pandian, proposed a wireless sensor network for wearable physiological monitoring systems to be used as an array of sensors integrated into the fabric of the wearer to continuously acquire and transmit the physiological data to a remote monitoring station. Then the data is correlated to study the overall health status of the wearer. The use of physiological sensors with miniaturized electronics is to condition, process, digitize and wireless transmission integrated into the single module. These sensors are strategically placed at various locations on the vest.

In [9], Qiu et al. proposed an authentication protocol using Loran signal. Loran is a low frequency pulsed navigation system. It can make resistant to unauthorized uses and tampering. Therefore, a signal authentication protocol, called (TESLA), is proposed and implemented. The result shows that (TESLA) provides strong protection against location spoofing.

My contribution

General view of security reveals that the secret things are strong with moving objects rather than fixed things where the result of continuous movement and change the location present the success of the current proposed idea showing excellent results of its implementation.

The protocol presented in this thesis is independent of the actual localization technique.

However, in the current proposal, the dynamic location of the mobile node and the dynamic tolerance distance can be used with both fixed and mobile applications. The real advantage of our proposal over the previous proposals is that it performs well with high speeds mobile where the successful rate of decryption exist with accepted result compared with previous work where they have had success in the state when the velocity is low and doesn’t exceed 30 km | h. And the increase in the velocity causes a decrease in the successful rate of decryption till reaching zero.
In addition, the DTD function changes with the speed which makes our suggestion very strong and the results are reasonable enough for our strongest solution.
Also the mobility and the frequent change in location make this protocol very strong against attacks.

Chapter 3

The Proposed Solution

Dynamic Location-based encryption research often attempts to answer one of the following questions:

- How is data encrypted using dynamic location?
- How the speed is related to the path movement?
- How to make the interval of encryption/decryption more practical with dynamic location?
- And, how to produce more accurate results than the results of the previous solutions?

However, to detect mobile location is subject to additional research problems. These problems can be expressed by the following questions:

- How to detect mobile location?
- How to get location parameters?
- What advantages and disadvantages exist in mobile application/services location?
- And, how to solve these disadvantages.

The overall approach of this thesis is to apply dynamic location using existing location services in mobile phone described in (Appendix A) and its equivalent dynamic tolerance distance (DTD) and speed to generate secret key which applied to encrypt/decrypt data sent between mobile phone. It aims to generate a secret key which protect the data sent between mobile phones where the spy and spoofing have become major threats to the confidential data.

This chapter is divided into four sections that attempt to answer the following questions:

- What is the general perspective for development?

- What are the details descriptions of the proposed solutions? (Section 1)
- How to make possible location to generate the secret key? (section2)
- What are the properties and advantages of the proposed solution? (Section 3)
- What are the disadvantages of the proposed solutions? (Section 4)

3.1 Description of Proposed solution

The proposed solution is to generate a secret key shown in (Figure 3-1) based on the parameter generated by the location of mobile and dynamic tolerance distance (DTD). the process is divide into two parts; the receiver part and the sender part. The right part, represents the mobile phone receiver and the left part, represents the mobile phone sender as it is shown in Figure 3-1.

The receiver mobile generates the secret key by reading a set of coordinates during the movement. This movement depends on its speed to find the equation of path function and then calculates the estimated coordinate after a fixed time related to its speed. Moreover, it calculates the DTD to increase its practicality in the interval of encryption / decryption of the data, because the location service receiver has problem in inaccuracy and inconsistently which differ in the type of location service in the device. The details of generation secret key are given in the next section. In addition, it generates R- key randomly with the same length of secret key, therefore it gets the final key through XOR between the Secret key and the R-key.

After that, the receiver mobile sends the parameter generated on the proposed algorithm and the R-key which are the plaintext given in the figure3-1 to the sender using encrypted SMS by the public key through the asymmetric encryption. When the sender receives an encrypted SMS message, it decrypts using the private key. The sender generates the secret key using the decrypted parameter from the SMS and determines the final key whereas the XOR between the secret key and the R-key.

This final key is used in the symmetric algorithm to encrypt the message sent from the sender to the receiver. The receiver decrypts the message using its final key in the symmetric decryption.

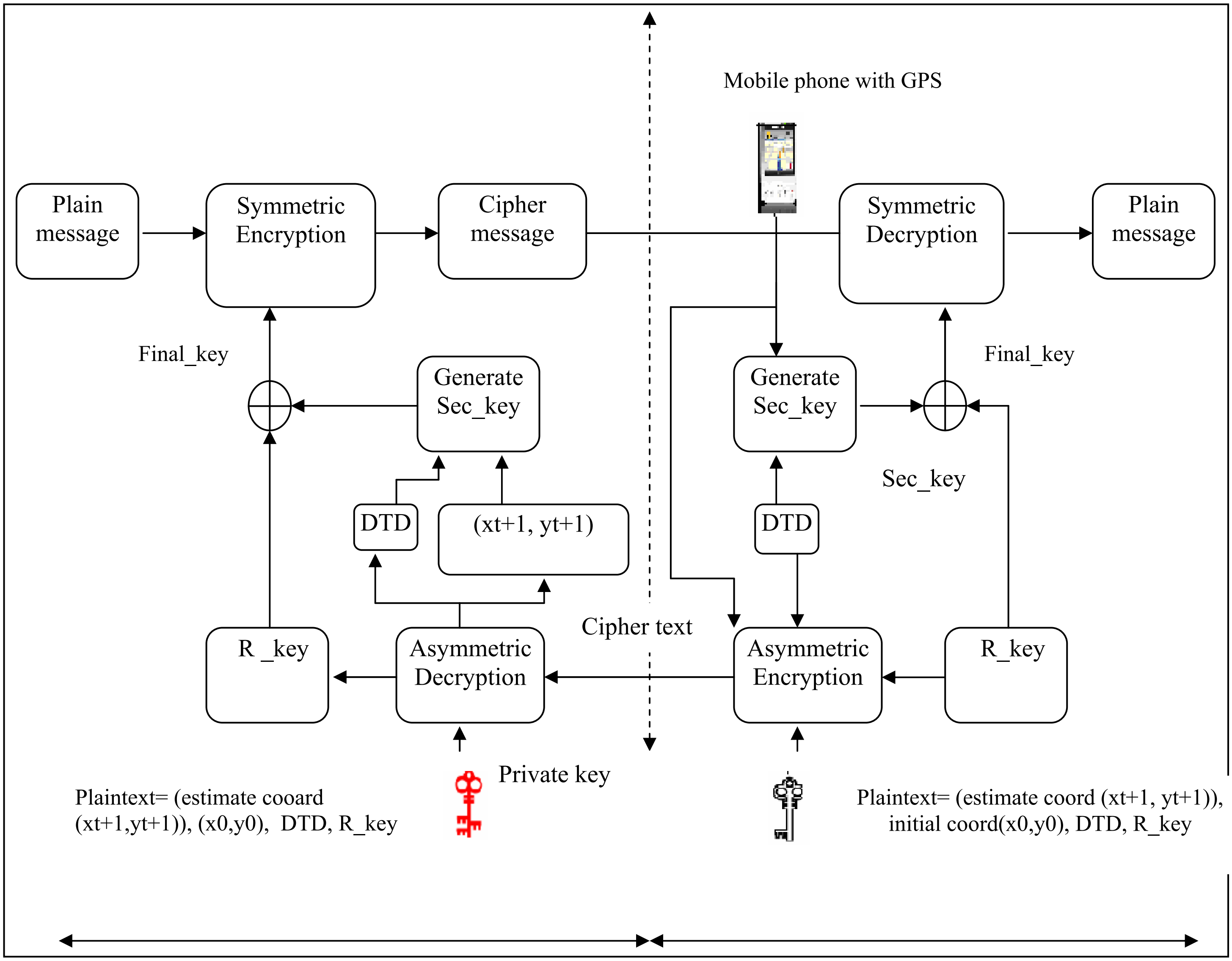


Figure 3-1: Generation process of secret key

The generation of the secret key consists of the following parameters:

- The initial coordinate in the current location.
- Estimate coordinate, is the expected location at receiving time.
- Dynamic tolerance distance DTD.

- And, the R-key, is the random key.

To compute the estimated coordinate, the study of the path movement of the mobile phone must be studied. So, the mobile phone reads some coordinate during movement.

It is supposed that the receiver mobile starts at time t_0 at a location as its longitude and latitude values are $L_0(X_0,Y_0)$ which is the initial coordinate read in the path.

The mobile phone receives reading at time (t) is L_t (X_t,Y_t) with $t = t_1, t_2, t_3, . .$ Such that $t_i = t_0 + i*d$ where d is a fixed time unit interval with arbitrary but known value.

The movement of the mobile device itself is arbitrary in any direction and any velocity means that its movement is not uniform.

The generation of the secret key requires computing an estimated coordinate expected after a certain time. So, the next position of coordinate is given by the following equations according to the Movement Law [Newton Low]:

$x-x_0 = v_x*t+ (1/2)*a*t^2$

$y-y_0 =v_y*t +(1/2)*a*t^2$

$v_{x-} = v_{0x} *\cos \theta$

$v_{y-} = v_{0y} *\sin \theta$

So,

$$x_i=x_{i-1}+(v*t +(1/2)*a*t^2)* \cos \theta \qquad (3\text{-}1)$$

$$y_i=y_{i-1}+(v*t +(1/2)*a*t^2)* \sin \theta \qquad (3\text{-}2)$$

Where a is the acceleration and v is the velocity of the $(x_{i-1,}\ y_{i-1})$ coordinate.

Generally, the path equation is a polynomial function given by:

$$(\Delta) :\{y(t)=a_n*x_n(t) +a_{n-1}*x_{n-1}(t) + \dots a_1*x_1(t) +a_0 \qquad (3\text{-}3)$$

Each time, the mobile receiver reads the parameter "latitude, longitude and velocity", it does the following test:

- **If the value of velocity is not high** (v<100 km/h), it means that the distance of the next coordinate is very short because the period time is constant. So, its movement is uniform which makes the function of path (Δ) in (3-3) linear (n=1)

(Δ): $y(t) = a_1 * x(t) + a0$

But if the velocity is high, the path equation follows the size of coordinate belongs to the path equation (Δ).

If most of the general coordinates belongs to a path, the path equation is linear:

$y(t) = a_1 * x(t) + a_0$

- **If the value of velocity is high** (v≥100 km/h), it finds a polynomial that fits those points.

For simplification, this polynomial is approximated to be cubic function with third degree (n=3). After selecting the appropriate path, which depends on the nature of the movement, the estimate coordinate is determined by computing the next coordinate used in the secret key.

At time t=t+1 the algorithm estimates the next position using equation (3-1) and (3-3)

$c_{t+1} = (x_{t+1}, y_{t+1})$

In : $x_{t+1} = x_0 + (v * t * + a * t^2) * \cos\theta$

θ is the angle between two coordinate as see in Figure3-3 given by:

$$\theta = \arctan\left(\frac{y_t - y_{t-1}}{x_t - x_{t-1}}\right) \qquad (3\text{-}4)$$

If the location services in mobile phone read the speed, then the receiver mobile reads its velocity directly from the mobile device. But if the device has not this service, it is determined directly from the Low of Velocity. The velocity equation is given by the following equation:

Velocity = Distance/Time

$$\Delta\vec{r} = \vec{r}_i - \vec{r}_{i-1} = (x_i - x_{i-1})\vec{i} + (y_i - y_{i-1})\vec{j}$$

The Distance r given by

$$|\vec{r}| = \sqrt{x_i - x_{i-1})^2 + (y_i - y_{i-1})^2}$$

Where "d" is a fixed time

So, the velocity v equals:

$$v = \frac{\sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2}}{d} \qquad (3\text{-}5)$$

Then, substituting the value of (x_{t+1}) in the path equation (Δ) of (3-3) gets (y_{t+1}).

In general, the path movement takes the ellipse form which is shown in Figure (3-2). That is because the coordinate is distributed inside the ellipse form as the explanation given in the top of this section, where the path function is changed through the change of speed. So, if the speed is not high or the path equation follows the size of coordinate belong to the path equation (Δ). The path function is linear. Then, some of this coordinate is arranged in a straight line but the rest of coordinate is arranged around the straight line. Also, if the speed is high the path function is polynomial and the coordinate is arranged in wide interval range. This coordinate in the two cases is distributed inside ellipse form Figure (3-3).

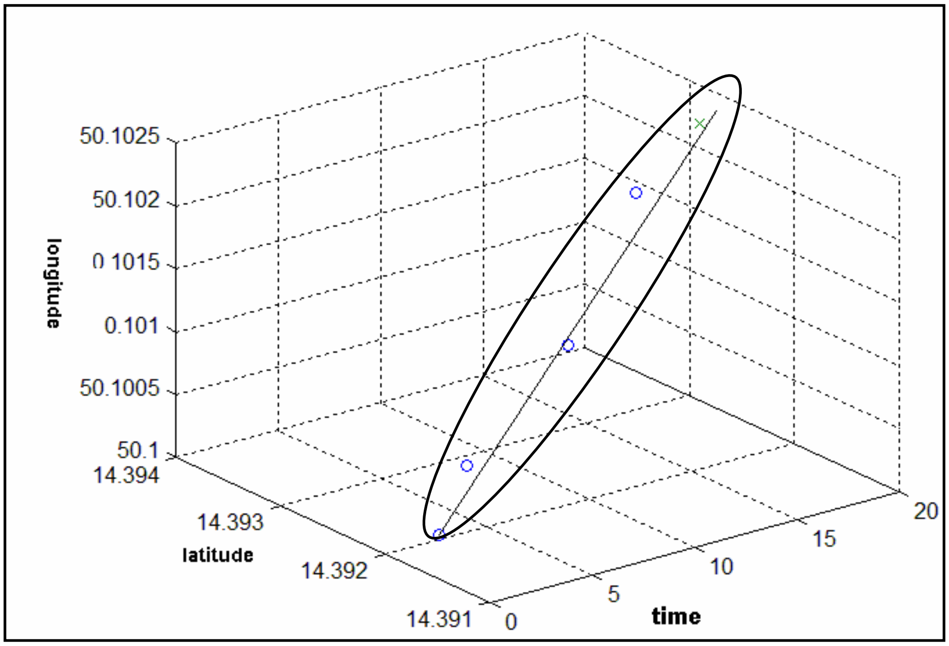


Figure 3-2: Distribution of Coordinate in Ellipse Shaped with low Velocity.

After calculating the estimate coordinate, it is applied to generate the secret key.

This coordinate is multiplied by (10,000) to be an integer value because the mobile devise reads the coordinates as following example:

Latitude: $31^{0}32^{'}29, 31''$N

This latitude equals to N 3132.2931, (N) means the north.

Longitude: $34^{0}29^{'}27, 49^{''}$E

This longitude equal to E 3429.2749, (E) means the east.

This makes the coordinate be an integer by multiplying by (10,000) to get X_t, Y_t

X_t = latitude* 10,000 = N 3132.2931* 10,000

Y_t = longitude* 10,000 = E 3429.2749 *10,000

So, Xt = N 31322931 and Y_t = E 34292749

From the estimation of CoordTrans tool of Franson Company, the values are (6) and (5.4) for latitude and longitude corresponding to 1 m [2]. This coordinate is converted to meter by dividing X_t into (6) and Y_t into (5.4) to get $x_t = X_t/6$ and $y_t = Y_t/5.4$

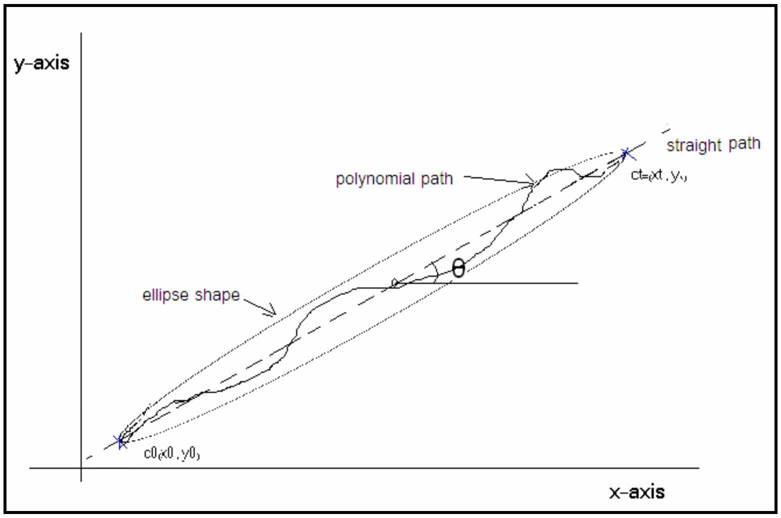


Figure 3-3: Ellipse Shaped in the Path Movement.

The second parameter is the dynamic tolerance distance (DTD). A dynamic Toleration Distance (DTD) is designed to increase its practicality in the interval used to encrypt or decrypt the data because the location service receiver has a problem in inaccuracy and inconsistent differs in the type of location service where the result of X_t and Y_t are divided by (DTD). DTD is the allowed region range in which the decrypted can done successfully where the DTD function is calculated as follows:

- the last coordinate that has been read in the path movement is taken as a center of the circle in which its radius is the length of the distance between this coordinate and the expected one. Therefore the DTD distance would be within the validate selected arc angle α which present a circle with the center is the estimated coordinate (x_e,y_e) and the radius is the DTD distance - as shown in Figure 3-4

DTD is the surface inside this circle. DTD distance= R_{DTD} is varying and depending on velocity and the angle α by the following equation:

The length of distance $|\vec{r}| = \sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2}$

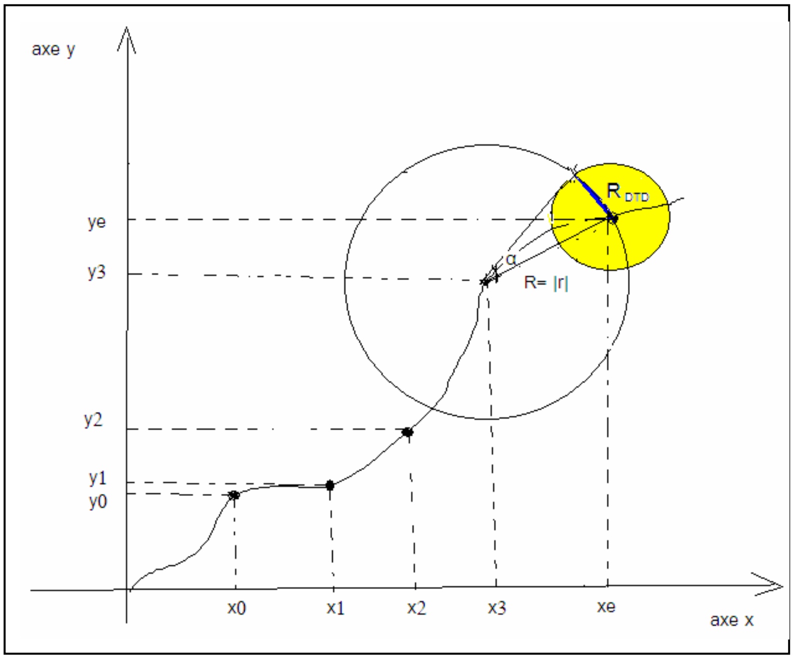


Figure 3-4: The dynamic tolerance distance (DTD) range

$|\vec{r}|$ = v*t, because the movement is uniform

So, $R_{DTD} = |\vec{r}| * \tan\alpha$

Then,

$R_{DTD} = v*t*\tan\alpha$ (6)

The DTD is the surface of circle which equal

$DTD = \Pi * (R_{DTD})^2$

$DTD = \Pi * v^2 * t^2 * (\tan\alpha)^2$

The table 3-1 summarizes the values of the dynamic tolerance distance (DTD) for different velocities for different values of angle α and constant time. Take the time $t = t_i - t_{i-1} = d = 5s$

Table 3-1: Dynamic tolerance distance (DTD) vs. velocity for different values of α and with (t=5s)

	V=0 km/h	V=10 km/h	V=20 km/h	V=30 km/h	V=40 km/h	V=50 km/h	V=60 km/h	V=70 km/h	V=80 km/h	V=90 km/h	V=100 km/h	V=120 km/h
α= 0˙	0m	0m	0m	0m	0m	0m	0m	0m	0m	0m	0m	0m
α= 5˙	0m	1.47m	2.95m	4.42m	5.9m	7.38m	8.85m	10.33m	11.81m	13.28m	14.76m	17.71m
α=10˙	0m	2.44m	4.89m	7.34m	9.79	12.24m	14.69m	17.42m	19.59m	22.04m	24.48m	29.38m
α=15˙	0m	3.72m	7.44m	11.16m	14.88m	18.6m	22.32m	26.05m	29.77m	33.49m	37.21m	44.t65m
α=20˙	0m	5.05m	10.11m	15.16m	20.22m	25.27m	30.33m	35.38m	40.44m	45.49m	50.55m	60.66m
α=25˙	0m	6.47m	12.95m	19.42m	25.9m	32.38m	38.85m	45.33m	51.81m	58.28m	64.76m	77.71m
α=30˙	0m	8.01m	16.03m	24.05m	32.07m	40.09m	48.11m	56.13m	64.15m	72.16m	80.17m	96.22m

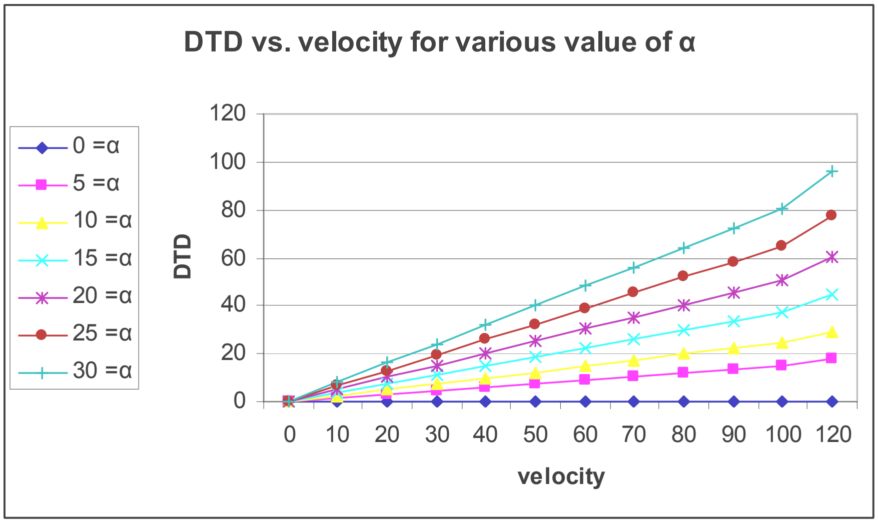


Figure 3-5: The DTD versus velocity for various values of **α**

From Figure 3-5 above, we can depict that if the velocity is very high, the R_{DTD} increases therefore the angle α must be very small to get less range of decryption. However, if the velocity is lower, the R_{DTD} decreases than the angle α must be increased at just to get existing and less range of decryption.

3.1.1 Practical Example to compute the estimate coordinate and DTD

The following example is taken from the emulator of J2ME Software where mobile phone registers the following coordinate through their movement:

Input: $c_i(x_i.y_i)$,t_0,d,v_i where $0<i<n$

Let $t_i=t_0+i*d$

For n=4, d=5s

t_4=[0, 5, 10,15]

Lat1: x_0 = 14.391490311821090

Lon1: y_0= 50.1003507324937160

V1= 100km/h

Lat2: 14.392198992161640

Lon2: 50.100411168118760

V2= 89km/h

So, v_i is the speed of last coordinate, here the speed is v_3=89km/h

Since, v < 100km/h, the path equation is a linear function

For t3 =10s

Substitute in the path function to get the estimate coordinate $c_3=(x_3,y_3)$

Latest: x_3= 14.3922821057696080

Lonest: y_3= 50.1009891199275540

$R_{DTD} = v*t*\tan \alpha$

$R_{DTD} = 17.7182$ meter

3.1.2 The Algorithm for generation the parameter in the secret key

Step 1: "The path Equation"

```
Input:  fixed period time: d, number of coordinate: n, initial time: $t_0$
For   $0 < i < n-1$
Read the coordinate: $c_i(x(t_i), y(t_i))$
$x_i (t) = x(t_i)*10000/6$                 ; latitude in meter
$y_i (t) = y (t_i)*10000/5.4$              ; longitude in meter
        If the velocity exist
         Read $v(t_i)$
              else
             Compute $v(t_i)$ according to the following equation
             $V_i(t)= \frac{\sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2}}{d}$
             sleep d
             $t_i= t_0 +d*i$, i =i+1
             end
    If $v_{n-1}<100$km/h                ; the last velocity for last coordinate read it in the path
    Then (Δ) $y(t) =a_1*x(t) +a_0$       ; the path function is linear
     else
    (Δ)= {$y(t)=a_n*x_n(t)+a_{n-1}*x_{n-1}(t)+..+a_1*x(t)+a_0$}
                                        ; as example n=3 the path function is cubic
```

```
Let A = [$a_1,a_2,\ldots a_n$]          ; is a set of all points are registered through movement
    B = {am∈ A / am∈ (Δ)}    ; B is a set of points which lies on the curve (Δ)
If size (B) ≥ size (A)/2 Then
    f (A) = (Δ) $y(t) = a_1*x(t) + a_0$ ; the path function is linear
else
    f (A) = (Δ) {$y(t)=a_n*x_n(t)+a_{n-1}*x_{n-1}(t)+..+a_1*x(t)+a_0$}
                                        ; as example n=3 the path function is cubic
End if
End
```

<u>Step 2: "The estimate coordinate"</u>

Let $v_{n-1}= v_n$; the velocity of the last coordinate equal to the estimate velocity

$t_n = t_0+d*n$

Compute θ according to the following equation

$$\theta = \arctan(\frac{y_i(t) - y_{i-1}(t)}{x_i(t) - x_{i-1}(t)})$$

$X_n (t)=x_o(t)+(v_{n-1}(t)*t_n* +a*t_n^2)* \cos\theta$

$Y_n=(\Delta(x_n))$; Δ is the path function

<u>Step 3: "Dynamic tolerance distance (DTD)"</u>

Input α

Let v= vi-1; the velocity of the last coordinate equal to the estimate velocity

t= d;

$R_{DTD} = v*t*\tan \alpha$

$DTD=\Pi* (R_{DTD})^2$

3.2Final key Generation

The final key is generated by the exclusive OR operation (XOR) between the secret key and the R-key given in Figure (3-6).

The proposed secret key mainly includes the estimated coordinates and (DTD) that are computed in the last section.

The steps to compute the secret key are as follows:

1. Enter the estimate coordinate (x_{t+1}, y_{t+1}) computed in the last section.
2. Multiply the estimate latitude by ($10{,}000/R_{DTD}*6$) and the longitude by ($10{,}000/ R_{DTD} *5.4$) to get integer value and the division by (6) in latitude and (5.4) in longitude to get the value of coordinate in meter and divided by (R_{DTD}) to get the coordinate in the interval of decryption [2].

The set of coordinates is generally included inside the ellipse shape that takes (x_0, y_0) and (x_{t+1}, y_{t+1}) is located on the perimeter of the ellipse as in Figure 3-3 above.

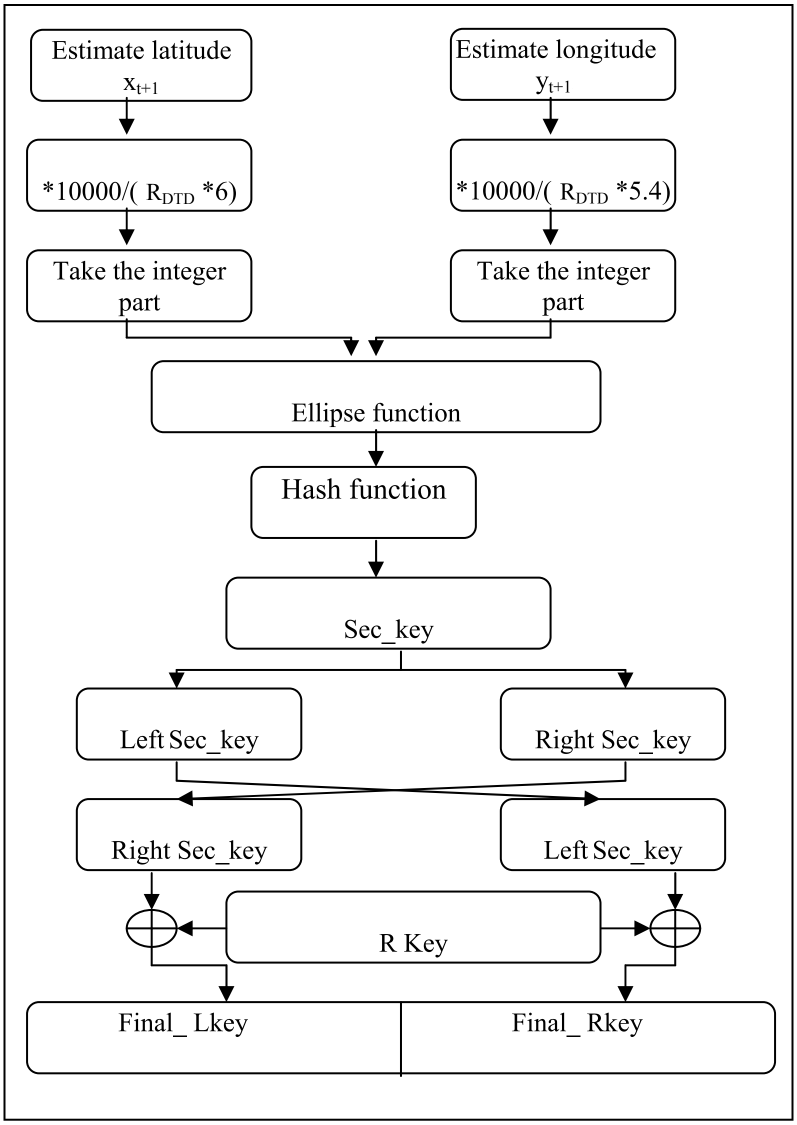


Figure 3-6: Generation of final key

- Ellipse function

From Figure (3-7) the new axes is given by

$x' = x\cos\theta - y\sin\theta$ (3-7)

$y' = x\sin\theta + y\cos\theta$

The function of ellipse is given by:

$$R(X,Y) = \left(\frac{x' - \bar{x}}{a}\right)^2 + \left(\frac{y' - \bar{y}}{b}\right)^2 = 1 \qquad (3\text{-}8)$$

Substitute (3-7) in (3-8) to get (3-9)

$$R(X,Y) = \left(\frac{X*\cos\theta - y*\sin\theta - \bar{x}}{a}\right)^2 + \left(\frac{x*\sin\theta + y*\cos\theta - \bar{y}}{b}\right)^2 = 1 \qquad (3\text{-}9)$$

Where

$$a = \frac{(x_{\max} - x_{\min})}{2}$$

$$b = \frac{(y_{\max} - y_{\min})}{2}$$

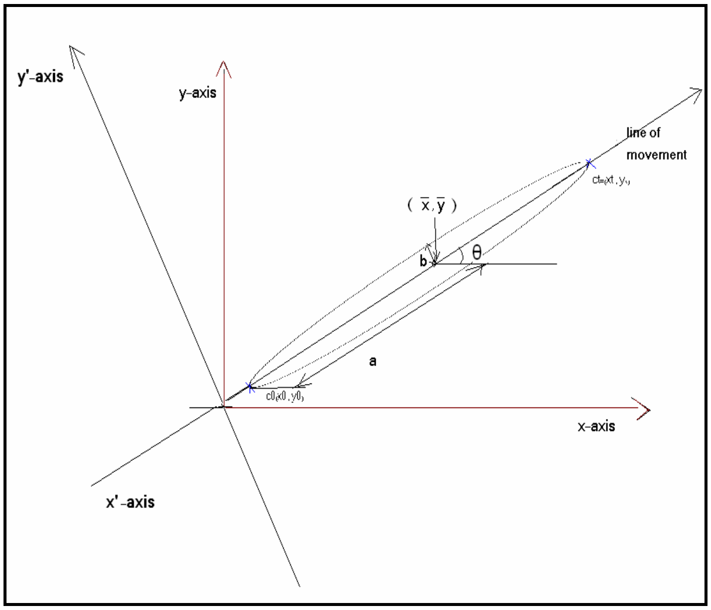


Figure 3-7: Moving the Ellipse form in New Axes

$$\bar{x} = \frac{x_{t+1}}{2}\cos\theta$$

$$\bar{y} = \frac{y_{t+1}}{2}\sin\theta$$

$$\theta = \arctan\left(\frac{y_t - y_{t-1}}{x_t - x_{t-1}}\right)$$

Substituting the estimate coordinate (x_{t+1}, y_{t+1}) in the ellipse function, then $R(x_{t+1}, y_{t+1}) = w$, (w) is fractional number. The result value from ellipse function applied in the hash function to get fixed length in hex decimal.

The (MD5) hash algorithm is utilized as example which generates a (128-bit) digested for the combined result where any hash function can be applied. The hash function is used to hide the resulting value of the ellipse function, which makes the secret key more strongly because the result value of elliptic function is a fractional number.

Then, the digest is split into two (64-bit) values then swapped to complicate the sec-keys. This step causes that the target coordinate is unable to be derived from the sec_key.

The R-key are generated randomly.

So, using (XOR) function between the secret key left (secL_key) and the random key (R_key) with 64 bit, to get the final key left.

Moreover, by using (XOR) function between the secret key right (secR_key) and the random key (R_key) with 64 bit to get the final key right. Then the merge between these two keys to get the final key.

Final_Lkey = R_key xor secL_key and

Final_Rkey = R_key xor secR_key

Final _key = Final_Lkey && Final_Rkey

3.2.1 Example of generation final key

By applying our previous algorithm an example to generate final key is demonstrated in Figure 3-8

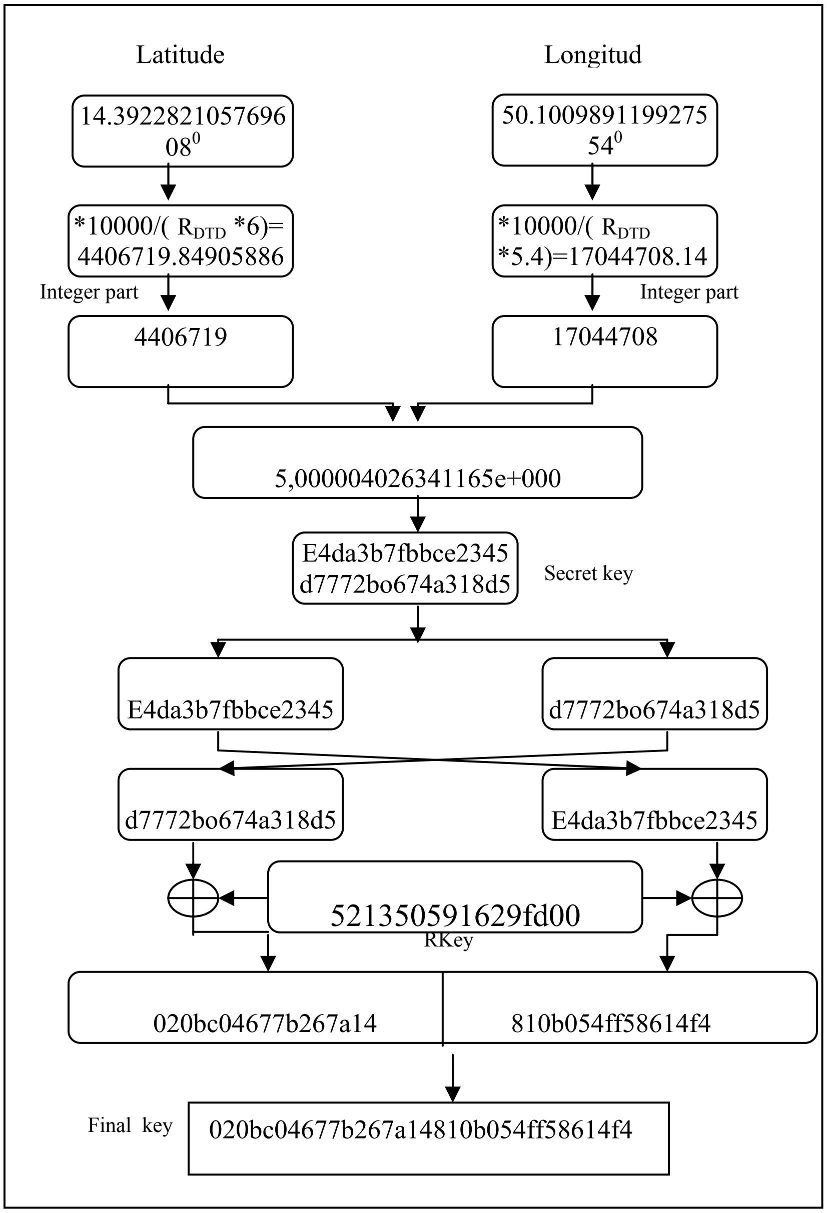


Figure 3-8: Example to generate final-key

In the practical implementation, (AES) is used in symmetric encryption algorithm and RSA in asymmetric encryption algorithm (Appendix B.1, B2).

3.3 Properties of The Proposed System

There are several advantages of the current proposal resumed in several points. The use of dynamic location with speed coefficient improves the confidentiality of the coordinates and the increase in speed increases the range of (DTD) which makes the percentage range of decryption succeed. This increases the efficiency and the perfection of the secret key compared with the previous solutions.

The availability of location service in mobile phone increases the facility of implementation especially with devices symbian (S60) or modern devices were are more precise and stronger in use and this increases the effectiveness of the proposal. This makes the advantages of the device is more likely to attack and the proposal is the best solution to solve this problem. The accuracy of modern appliances in the presence of combination of different location techniques such as being capable of using a hybrid method of geo-location interface with (GSM), (Wi-Fi) and (GPS) receiver, and this increases the flexibility of application and data confidentiality. Besides, the possibility of introducing coordinates manually or using the internet in countries that provides this service at free or little cost.

In addition to the abovementioned, the strength of key depends on the dynamic path for the receiver (MN) and (DTD). Therefore, the probability to break the secret key is impossible because no one knows the estimate coordinate since it is not yet at this position and the change in velocity makes the range of decryption less than static method. Also, (DTD) can be a fractional number with small interval which makes the key more secured. The random key and the initial coordinate are incorporated by the secret key which makes the final key very strong.

3.4 Disadvantages of This System

Some of the advantages of this system have corresponding disadvantages. It means that the disadvantage of the key is the difficulty in reading the coordinates according to available service and device. For example, if the weather is cloudy or the devise is in door, the reading of coordinates is difficult or non-existent if the device has the (GPS) location services and this makes the device accessing the internet to read its coordinates. But this method is costly than use the previous registered coordinates in the device. This method is not secured specially if the device is stolen or lost even for a short time.

Other disadvantages is, if an attack has become on the private key in the case of sending (SMS) transactions such as man in the middle which makes it easier to penetrate the messages easily.

Chapter 4

Practical implementation

In this chapter, the proposed algorithm is implemented using J2ME software to demonstrate the claimed advantages of our proposal.

This chapter is divided into four sections organized as follows:

After giving an overview of the J2ME software algorithm in section (4.1), we have come up with the experimental study in section (4.2) which demonstrates the implementation steps of the proposal solution. In section (4.3), the security analysis of the experimental results is tested in different types of data. Also some examples of (MMS) messages are sent in real time using mobile phone and by simulation using emulator which is given in section (4.4) in the last section. An example in real time is given to test the effectiveness and strength of the proposal algorithm and compared by previous solutions.

4.1 J2ME Software

Java (2), Java Platform, Micro Edition (Java ME) (J2ME) are Sun's version of Java designed for small devices with a small memory size little as (128KB) of (RAM) and limited processors are powerless than those used on typical desktop and server machines such as (PDAs), cell phones, and other consumer electronic and embedded devices [66,67].

J2ME is actually consists of a set of profiles. Each profile is defined for a particular type of device and consists of a minimum set of class libraries required for the particular type of device and specification of a Java virtual machine required to support the device. The virtual machine which specified in this profile is not necessarily the same as the virtual machine used in Java 2 Standard Edition (J2SE) and Java 2 Enterprise Edition (J2EE).

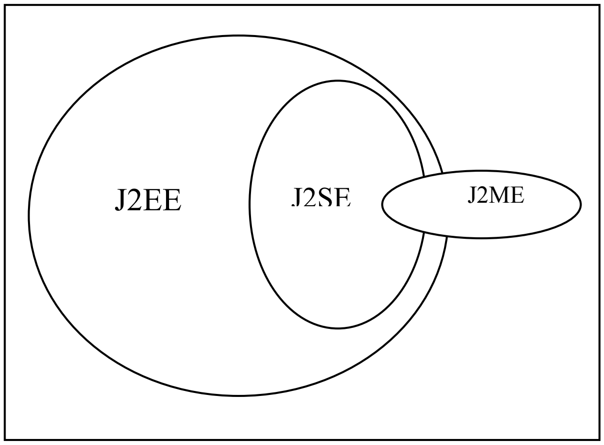


Figure 4-1: The three Java editor

J2ME is a robust and flexible environment for the applications running on mobile phone and other embedded devices [65]; J2ME architecture contains three layers which are [33]:

1. **The Java Virtual Machine (JVM):**

It includes a set of (APIs) and a virtual machine that is designed in a modular fashion allowing for scalability among a wide range of devices. The Virtual Machine (VM) supports the Configuration Layer by providing an interface to the host operating system.

2. **Configuration Layer:**

It has two possible configurations [33, 65ch2]; (CLDC) Connected Limited Device Configuration used for small, resource-constrained devices such as cell phones and low-end PDAs and (CDC) Connected Device Configuration used for big and powerful devices like high-end PDAs

3. **Profile Layer:**

It is a specification of the phone and services that can be applied on the mobile phone. The most popular profile is the (MIDP) Mobile Information Device Profile.

In particular phone devices J2ME technology made up of (MIDP) Profiles and (CLDC) configuration. And both (MIDP) and (CLDC) are libraries helping to build and constructing the application. (MIDP) versions vary from phone to other with the latest version like (MIDP 2.2.) and the difference between the versions that they contain new libraries.

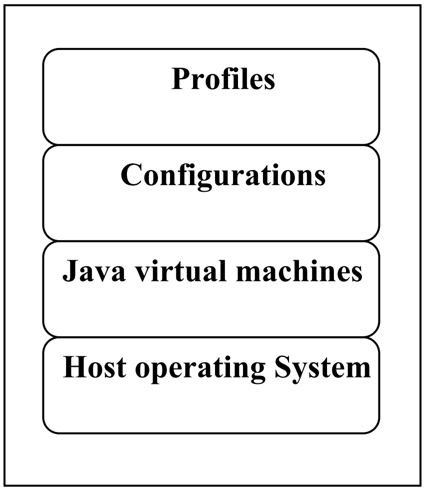


Figure 4-2: J2ME architecture

The application in this study focuses on developing J2ME application for mobile phone with J2ME running environment (CLDC) configuration and (MIDP) profile. The application of J2ME software runs the emulator in different models of mobiles takes the form of a hardware device. The emulator allows us to develop, test, and debug mobile applications before downloading them to the mobile.
A popular use of emulators is much more like the real device and to mimic the experience of running the application written in personal computers. Emulating these on modern desktop computers is usually less cumbersome and more reliable than relying on the original machines, which are often expensive and hard to find.

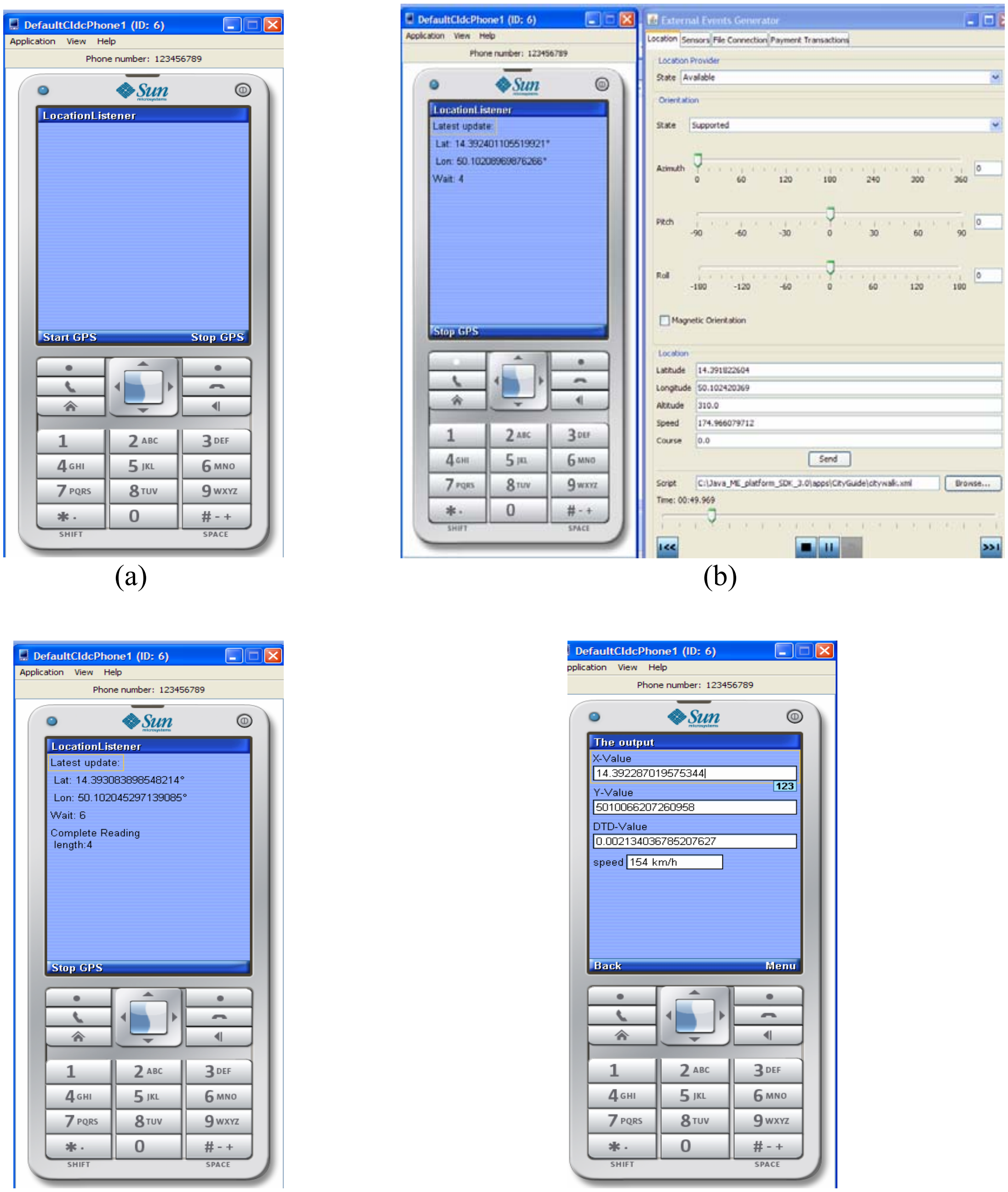
4.2 Experimental Study

4.2.1 Experiment 1

A. <u>Detect the Location and Coordinate of Mobile Phone Using GPS:</u>

Location program is designed to runs location services /application in the device where it log a certain number of coordinates and speed through the emulator or mobile device. The steps are given in Figures 4-3.

In Figure 4-3.a, GPS button is pressed start. Figure 4-3.b, is the start read numbers of coordinates and velocity from (GPS) emulator. After given time as in Figure 4-3.c, the registration completed by pressing stop GPS. The estimate coordinate, (DTD) and speed are treated and presented in Figure 4-3.d.



(a)

(b)

Latest update:
Lat: 14.392401105519921°
Lon: 50.10208969876266°
Wait: 4

State: Available

State: Supported

Azimuth: 0

Pitch: 0

Roll: 0

☐ Magnetic Orientation

Latitude: 14.391822604

Longitude: 50.102420369

Altitude: 310.0

Speed: 174.966079712

Course: 0.0

Script: C:\Java_ME_platform_SDK_3.0\apps\CityGuide\citywalk.xml

Time: 00:49.969

(c)

Latest update:
Lat: 14.393083898548214°
Lon: 50.102045297139085°
Wait: 6
Complete Reading
length:4

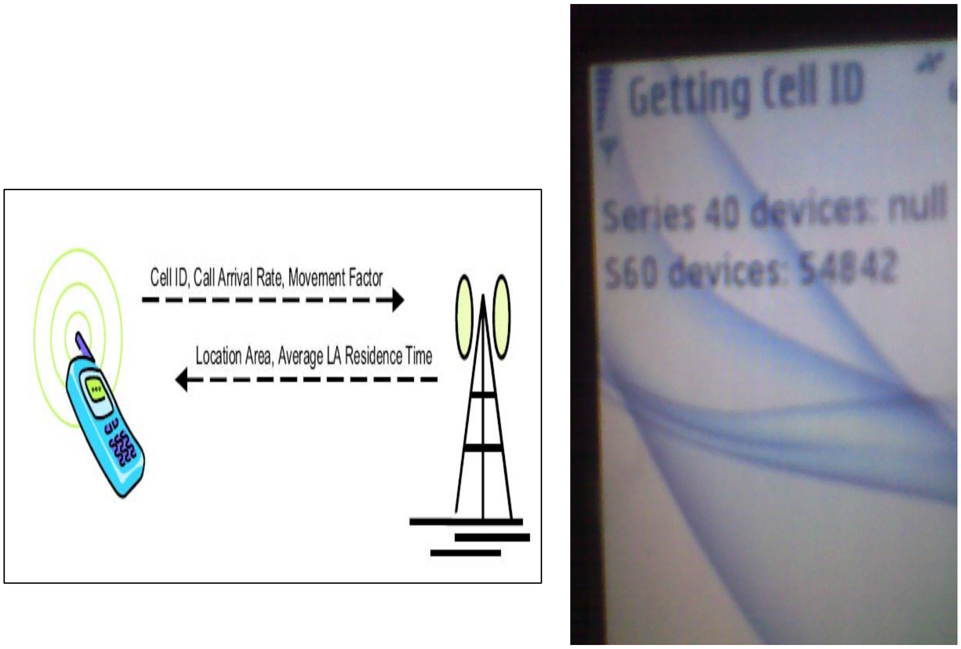
(d)

The output
X-Value
14.392287019575344
Y-Value
5010066207260958
DTD-Value
0.002134036785207627
speed 154 km/h

Figures 4-3: Steps to generate the estimate coordinate

B. Detect the Location and Coordinate of Mobile Phone Using Cell ID:

Location using Cell-ID is suitable only for mobile phones with series (S60) which is shown in Figure (4-4). This application lets the user know which Cell-ID is nearer and from this information it can approximately be known where the coordinate of the device consequently can be read from the map.


Cell ID, Call Arrival Rate, Movement Factor
Location Area, Average LA Residence Time

Getting Cell ID

Series 40 devices: null

S60 devices: 54842

(a) [15] **(b)**

Figure 4-4: (a,b) Detect mobile location using Cell-ID

4.2.2 Experiment 2

1. Generation of final key:

The data registered in the previous experiment is processed to compute the following parameters:

- *The initial coordinate (x_0,y_0);* which is the first coordinate started to be read by the location devise.

- *The estimate coordinate (x_{t+1}, y_{t+1});* which is the coordinate calculated in the algorithm after given time, dynamic tolerance distance (DTD) and the random key(R-key).

These parameters are used to generate the final key described in the algorithm in chapter 3.

The final key is applied in the symmetric key which used to encrypt/decrypt all types of data in plain message like texts, images, sound and video.

The creation of the final key is through the recipient when the sender informs the recipient about his intention to send him an encrypted message. The recipient directly starts to read his coordinates in fixed time through his movement path and generate the parameter using the algorithm in chapter 3, and then send it to the sender in encrypted (SMS) using public key in asymmetric encryption algorithm. The sender decrypts this encrypted (SMS) message using the private key.

Now the sender has the parameters that will be used to generate the final key which is used to encrypt the message that the sender wants to send to the recipient.

Description of Asymetric algorithm

As descripted in the previous section, the receiver records the following data:

- The initial coordinate $c_0(x_0,y_0)$, the estimate coordinate $c_t(x_t,y_t)$, (DTD) and R-key they will be transmitted via asymmetric encryption algorithm.

Through out the experiment, the (RSA) asymmetric algorithm is implemented which is used to encrypt the previous parameters used to generate the final key.

The public key is insecured key which is used to encrypt the data generated by the receiver mentioned earlier. When the sender receives the message, he decrypts it using privet key. An example of encrypting /decrypting, the parametrers generated by the receipient using (RSA) asymmetric algorithm given in appendix C at section C1.

1.1 The Encryption part:

- The symmetric key algorithm (AES) is used to encrypt the plain message by applying the final key which is the output of the XOR operation between the secret key and the R-key.

- The parameters that are decrypted by the private key in the asymmetric algorithm from the (SMS) messages are used to generate the final key by the sender to encrypt the plain message in symmetric key.

1.2 The Decryption part:

The cipher message is decrypted using the symmetric final key (AES) that are generated from receiver by calculating the following parameters by the algorithm as described in chapter3:

(The initial coordinate(x_0,y_0), the estimate coordinate (x_{t+1}, y_{t+1}), DTD, R-key)

The results obtained from the simulation to encrypt/ decrypt data using J2ME software are shown in Figure C-4 in appendix C.

In Figure (C-4.a), the user chooses encrypt button to encrypt the plaintext. By typing next, the input information is shown in Figure (C-4.b). After the Encrypt button is pressed in Figure (C-4.c), the plaintext file is encrypted as shown in Figure (C-4.d).

In Figure (C-4.e), the user chooses the decryption option. After the Decryption button is pressed, the user detects the estimated coordinate and Dynamic Toleration Distance (DTD) as in Figure (C-4.f). Then by pressing the button, the cipher message file is decrypted as shown in Figure (C-4.g). This means: "Open the folder to see the decryption file". If the acquired coordinate meets the constraint of target coordinate and (DTD), the content of the decryption file is the same as the plaintext file which is saved in the folder as shown in Figure (C-4.h). Otherwise, the content is indiscriminate and meaningless.

4.3 Security Analysis:

Some experiments have been conducted to test the robustness of the proposed secret key against all kinds of known attacks, such as statistical and various brute force attacks. In this sub section, the security analysis of the proposed method discus the statistical analysis, and sensitivity analysis with respect to the key to prove that the proposed cryptosystem is secure against the most common attacks.

4.3.1 Key Sensitivity Test:

An ideal encryption procedure should be sensitive with respect to the final key, i.e., the change of a single bit in the key should produce a completely different encryption at any type of plain message ;text, image, sound, video and so on.

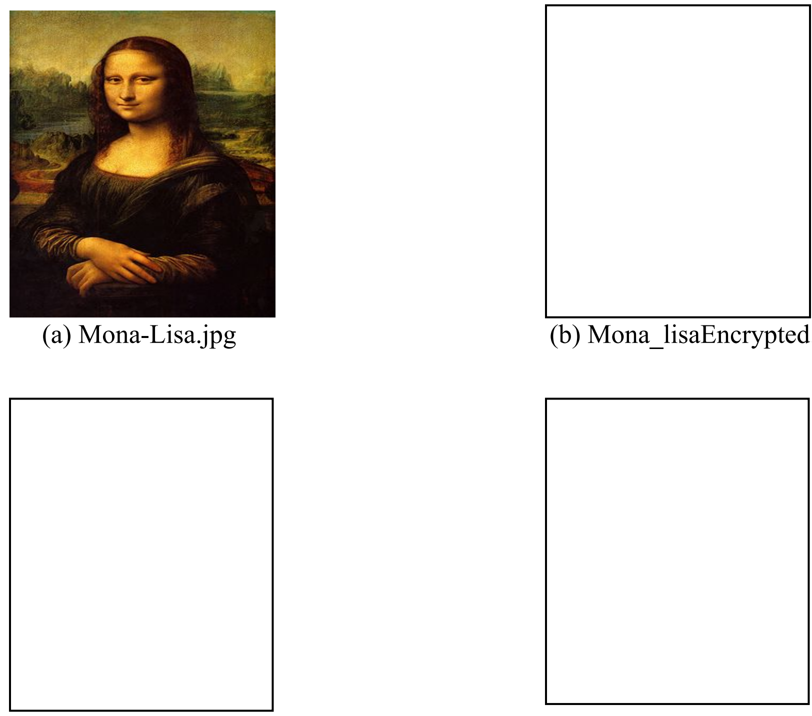
For testing the key sensitivity of the proposed encryption method, the following steps are performed:

1. An original image in Figure 4-5.a is encrypted by using the final key “ac963d95e449ea1cd409a3c34c8217c1 " (in hexadecimal) and the resultant ciphers are referred as encrypted image “cipher1’ as shown in Figure 4-5.b.

2. The same original message is encrypted by making slight modification in the final key i.e.“ac963d95e449ea1cd409a3c34c8217c2 "(the most significant bit is changed in the final key) and the resultant message is referred as encrypted image “cipher (2) “ in Figure 4-5.c.

3. Again, the same original message is encrypted by making slight modification in the final key i.e.”ad963d95e449ea1cd409a3c34c8217c1 " (the least significant bit is changed in the final key) and the resultant cipher is referred as encrypted image “cipher(3)” Figure 4-5.d.

With The same steps described above, it is applied to the plain text. The results are resumed as cipher-text, cipher-text1, cipher-text2 where shown in Appendix C



(a) Mona-Lisa.jpg (b) Mona_lisaEncrypted.jpg

(c) Mona_lisaEncrypted.jpg (d) Mona_lisaEncrypted.jpg

Figure 4-5: (a) plain-image (b) cipher1 (c) cipher2 (d) cipher3

To compare between the three encrypted messages cipher(1), cipher(2) and cipher(3) the correlation between them must be calculated, using the following equation [63,64].

The covariance equation is:

$$\sigma_{xy} = \text{cov}(x,y) = E[(x-\mu_x)(y-\mu_y)] = E[(x-E(x))(y-E(y))]$$

The correlation coefficient can be obtained by the equation:

$$\rho = r_{xy} = \sigma_{xy}/(\ \sigma_x\ \sigma_y\ ) = \text{cov}(x,y)/\ (\text{standard Dev}(x) * \text{standard Dev}(y))$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Where

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad , \qquad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 ,$$

So for comparison purpose, the correlation between the three encrypted messages is calculated, where (x) and (y) are the values of corresponding data in the two encrypted messages to be compared. In Tables 4-(1,2), the results of the correlation coefficients between the corresponding message of the three encrypted images cipher(1),cipher(2) and cipher(3) and the three cipher text , cipher text (1), cipher text(2) are presented.

Table 4-1: Correlation coefficients between the three different encrypted images obtained by using slightly different secret keys of the image shown in Fig. 4-5

Image 1	***Image 2***	***Correlation Coefficient***
Encrypted image cipher1 Fig. 4-5b	Encrypted image cipher2 Fig. 4-5c	0.0609
Encrypted image cipher1 Fig. 4-5b	Encrypted image cipher3 Fig. 4-5d	0.0625
Encrypted image cipher2 Fig. 4-5c	Encrypted image cipher3 Fig. 4-5d	0.0619

Table 4-2: Correlation coefficients between the three different encrypted texts obtained by using slightly different secret keys of the plain-text.

Text1	***Text2***	***Correlation Coefficient***
Encrypted text cipher-text	Encrypted text cipher-text1	0.0540
Encrypted text cipher-text	Encrypted text cipher-text2	-0.0337
Encrypted text cipher-text1	Encrypted text cipher-text2	0.0259

It is clear from the tables that no correlation exists among the three encrypted images and texts and even though these have been produced by using slightly different final keys.

Key sensitivity analysis shows that changing one bit in encryption key will result in a completely different cipher message.

Moreover, and in Figure 4-6, another experiment is conducted where attempt to decrypt an encrypted message with slightly different final key than the one used for the encryption of the original message.

The original image before encryption and the corresponding encrypted image produced using the final key “e8208a8993152bb45aa1bb7f0345444d” (in hexadecimal) are shown in Figure 4-6.a and Figure 4-6.b respectively. The decryption process has been performed twice. The first decrypted image (shown in Fig. 4-6.c) is encrypted with the final key “e8208a8993152bb45aa1bb7f0345444d” which is identical to the one used in encrypting the original one. On the other hand, the second image in Figure 4-6.d represents the decrypted image using the modified key “e8208a8993152bb54aa1bb7f0345444d” (in hexadecimal). It is clear that the decryption with a slightly different key, swapping 45 into 54 in the middle part of the key, fails completely and hence the proposed image encryption procedure is highly key sensitive.

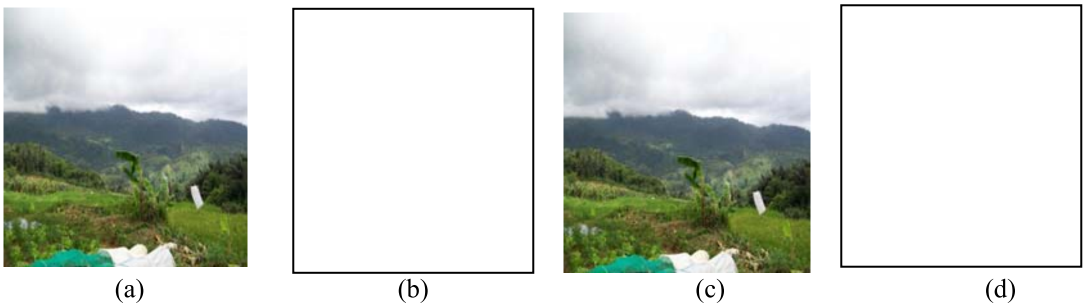


Figure 4-6: (a) Bandung-original image

(b) Encrypted image of (a)

(c) Decrypted image with the same final key of (b)

(d) Decrypted image with slightly different final key of (b)

4.3.2 Statistical Analysis:

The perfect cipher should be robust against any statistical attack. To prove the robustness of the proposed scheme, the statistical analysis are performed by calculating the histograms and the correlations coefficient in the plain message/ cipher message

- Histograms analysis:

Several examples for grey-scale/color images of dimension (m x n) and different sizes have been tested to calculate their histograms. Statistical analysis of Mona_Lisa and its encrypted image yield the histogram given in Figure 4-7. Other image examples are: cameraman, Bandung, Krakal-beach-Gunung-kidul and Oimg(2) images and their encrypted images are also yield their histograms which are given in appendix C at Figure (C-7). This figure shows that the histogram of the cipher images is completely different in which has no any presence in data or effect compared by the original image and hence does not provide any clue to employ any statistical attack on the proposed encryption procedure.

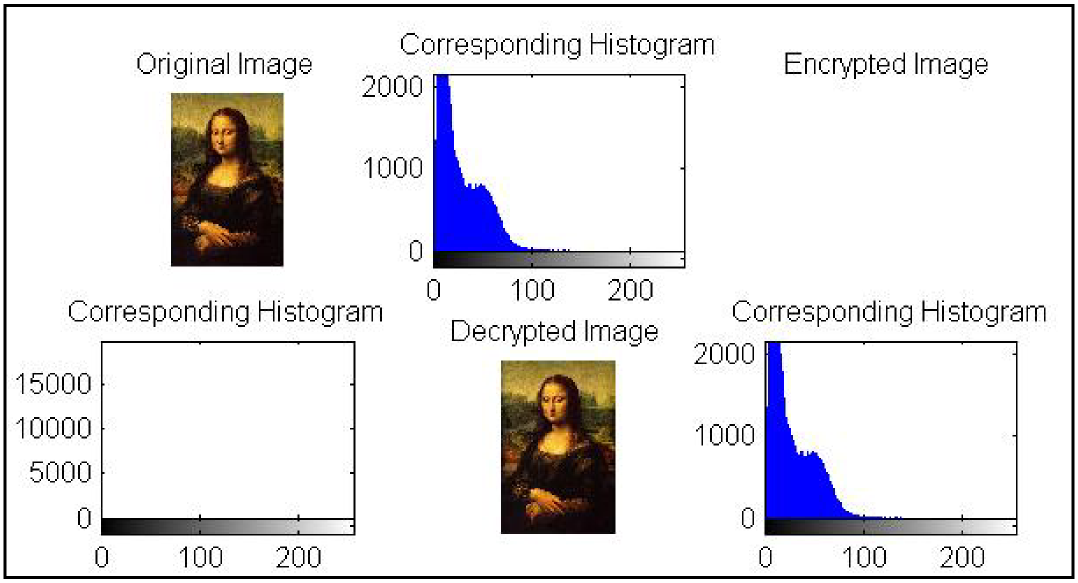


Figure 4-7 : Mona_Lisa image histogram

- Corrélation Coefficient Analysis:

In addition to the histogram analysis, the correlation between two images and texts (messages) in plain message/cipher message has also been analyzed respectively. The result is resumed in Table 4-3.

Also our results reveal that the correlation between the all (plain message and decryption Message) is equal to one. That means that the successful decryption operation with the proposed secret key.

From the results of this statistic analysis it demonstrates that the relation between secret encryption and cipher-data is of high complexity, and attacker cannot educe the encryption key from cipher-data.

Finally, the test on the histograms of the enciphered (decryption) data and on the correlations coefficient in the ciphered data showed that the proposed encryption algorithm is superior regarding the confusion and diffusion properties which strongly resist statistical attacks.

Table 4-3: Correlation coefficients between the plain message and cipher message

Plain-Image	Encrypted-Image	Correlation Coefficient
Cameraman Image	Cameraman encrypt Image	0.0698
Mona_liza Image	Mona liza encrypt Image	-0.0725
Bandung Image	Bandung encrypt Image	0.0390
Krakal-beach-gunung-kidul. Image	Krakal-beach-gunung-kidul encrypt Image	-0.0832
Oimg2 Image	Oimg2 encrypt Image	0.0148
Plain-Text	Cipher-Text	0.0540

4.3.3 Lossless and Opacity:

Clearly from the above experiments' results, we can note that the use of AES Symmetric encryption was lossless, since the decrypted message is exactly similar to the original message without any loss of data through encryption and decryption operations, which means that there is no recorded noise in the decrypted images which makes the protection of data more strong. It can also be noted that the opacity between the original images and the encrypted images is very high. In other words, the distortion between the original and encrypted images as shown in the above experiments is very high.

4.3.4 Duration time:

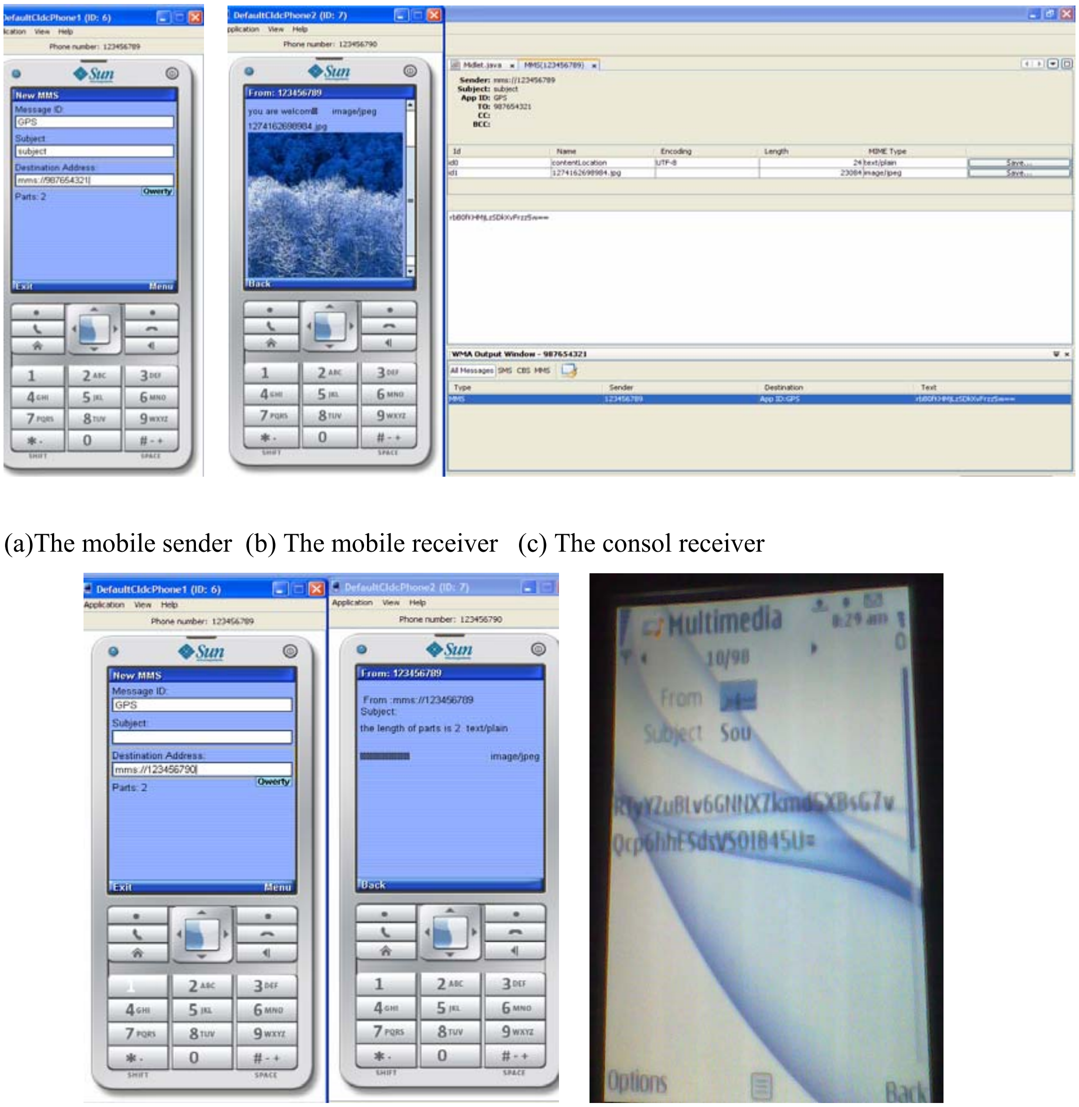
To measure the complexity of the proposed algorithm, the time in seconds for doing the encryption and decryption operations for the above experiments was recorded in Table 4-4.

Table 4-4: Encryption/Decryption speed test results of the proposed algorithm

Image	***Size***	***Encryption Time***	***Decryption Time***
Cameraman Image 804 x 553)	127KB	2.834000 seconds	2.664000 seconds
Monaliza Image (250 x 378)	20.4KB	1.373000 seconds	1.259000 seconds
Bandung Image(550 x 412)	30.2KB	1.401000 seconds	1.376000 seconds
Krakal-beach-gunung-kidul. Image (150 x 150)	4.83KB	0.98000 seconds	0. 95000 seconds
oimg2 Image (405 x 313)	12.1KB	1.195000 seconds	1.135000 seconds
Text	857B	0.8000	0.5000 seconds

4.4 Example of Sending MMS Using the Emulator:

The emulator with ID6 (123456789) in Figure 4-8.a sends MMS to the emulator with ID7 (123456790) with the same final key and to the WMA consol with ID (987654321) without secret key. The message in Figure 4-8b are decrypted successfully, but in Figure 4-8.c the message is cleared encrypted. The same MMS is sent to the emulator with ID 7 (123456790) and in real mobile but with different Secret key. The results are shown in Figure 4-8 (d, e). Other examples are presented in Appendix C in Fig C-5.and C-6



DefaultCldcPhone1 (ID: 6)
Phone number: 123456789
New MMS
Message ID: GPS
Subject: subject
Destination Address: mms://987654321
Parts: 2

DefaultCldcPhone2 (ID: 7)
Phone number: 123456790
From: 123456789
you are welcom▮ image/jpeg
1274162698984.jpg

Sender: mms://123456789
Subject: subject
App ID: GPS
TO: 987654321
CC:
BCC:

Id	Name	Encoding	Length	MIME Type
id0	contentLocation	UTF-8	24	text/plain
id1	1274162698984.jpg		23084	image/jpeg

rb80frHMjLzSDkXvFrzzSw==

WMA Output Window - 987654321

Type	Sender	Destination	Text
MMS	123456789	App ID:GPS	rb80frHMjLzSDkXvFrzzSw==

(a)The mobile sender (b) The mobile receiver (c) The consol receiver

DefaultCldcPhone1 (ID: 6)
Phone number: 123456789
New MMS
Message ID: GPS
Subject:
Destination Address: mms://123456790
Parts: 2

DefaultCldcPhone2 (ID: 7)
Phone number: 123456790
From: 123456789
From :mms://123456789
Subject:
the length of parts is 2 text/plain
image/jpeg

Multimedia
10/98
From
Subject Sou
RtyYZuBLv6GNNX7kmdGXBsG7v
Qcp6hhESdsVS01845U=

(d)The sender mobile (e) The receivers mobile (the key is out the range of DTD)

Figure 4-8 (a,b,c,d) example of sending MMS using the emulator and real mobile

4.5 Comparison of the Decryption Successful Rate between Dynamic and Static Location at Different Velocities:

an algorithm is implemented that encrypt and decrypt different types of data while moving by a car on the highway and streets of a subsidiary with different speeds. The effectiveness of the secret key in this algorithm is studied by taking the coordinates close to the estimated coordinates in the path.

The analytical study of the movement path at the receiver device with different speed can be summarized as follows:

For approximation a small range of DTD are choosed which is enough to guarantee successful decryption for any value of velocity, and for a specific value of $\alpha=15^0$.

- If the receiver device is moving slowly in a fixed time interval, then the motion path is a linear function and the expected point at time t+1 is located at the range of DTD which is increased by increasing the velocity.
- But, if it is moving with high speed, the motion path is a polynomial function and the range of (DTD) is higher than the previous case. In this study, it is supposed that the polynomial function is a third degree one where it takes the form of cubic function.

The same experiment was implemented for static secret key in the reference 2, where the results demonstrate that successful rate decryption is 100% at TD range and this rate decrease for extra distance (MD) which equal to (5 meter + TD) for very small velocity. In this experiment, the successful rate of decryption is studied at different values of velocity for extra distance (MD). The results show that the successful rate of decryption with different values of velocity in the dynamic case is much better than in the static case. This is clear from the Table4-4.

In static case: when speed = 0 the successful rate of decryption is in the range of MD. This ratio decrease to zero by increasing the speed, this is because the distance is proportional with the speed, considering that the range distance of decryption is almost constant, but the increase in the speed makes increase in the range of the distance which decreases the successful rate of decryption. This can be depicted from the Figure4-9.

But in the dynamic case, the velocity is proportional with DTD in which the DTD value increases by increasing the velocity. This is due to the increasing in the speed which makes the path movement non linear and increase the DTD range. So the increase in the speed causes another increase in DTD and that makes the successful rate of decryption high.

Also the decrease in the velocity makes the path movement linear which decreases the DTD range but in the range of decryption and that makes the successful rate of decryption also high. This demonstrates the strength of our protocol.

Table4-5: Successful Rate vs. Velocity for static and dynamic location.

Velocity(v)	**Successful rate for static location**	**Successful rate for dynamic location**
0 km/h	92%	92%
10 km/h	40%	89%
20 km/h	22%	85%
30 km/h	11%	77%
40 km/h	9%	75%
50 km/h	2%	73%
60 km/h	0%	69%
80 km/h	0%	67%
100 km/h	0%	61%
120 km/h	0%	63%

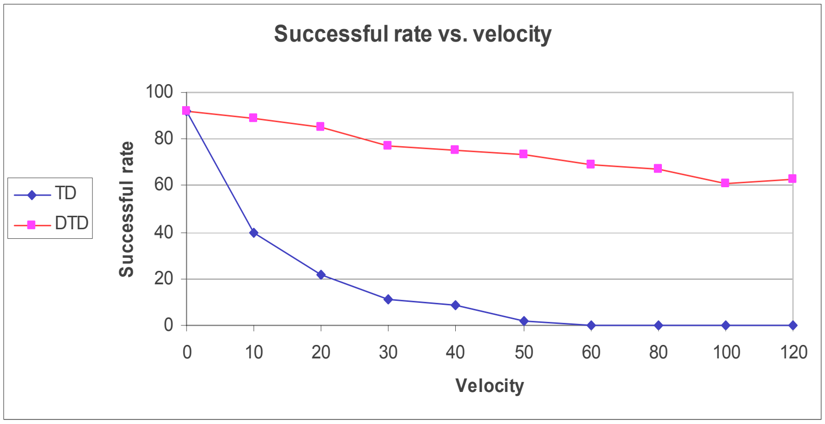


Figure 4-9: Comparison the successful rate between static (TD) and dynamic (DTD) location for various values of velocity

The advantage of our proposed algorithm depend on the DTD which is proportional with the velocity where the DTD function given by :

The radius of DTD (R_{DTD}) = v*t*tan(α) and the DTD = Π (R_{DTD} $)^2$ which is the surface of circle make the region of decryption successfully.

For different value of angle (α) the increase in velocity make increase in R_{DTD} and that increase the range of DTD, also the decrease in the velocity make decrease in R_{DTD} which decrease the range of DTD as given in figure 4-10 which demonstrated the dynamic state of our proposed algorithm

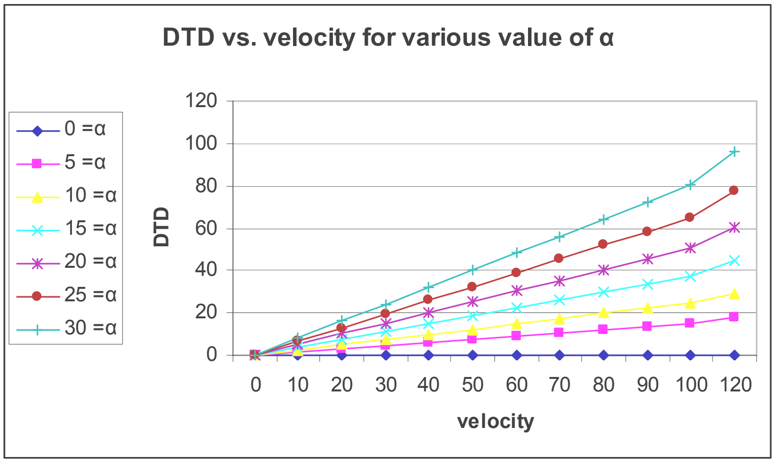


Figure 4-10 DTD vs. velocity for various value of angle (α)

Chapter 5

Conclusion

5.1 Concluding Remarks:

This thesis solves the attack problem through communication between mobile devises like the sending (MMS) and (SMS) message. The proposed solution is a new security algorithm that uses a complex secret key to encrypt all types of messages transmitted between mobile phones. This secret key is made from dynamic coordinate, dynamic tolerance distance (DTD) and velocity of Mobile phone. In this algorithm, a mobile receiver with location service, registers a set of coordinates and velocity during movement and estimates the next position. The algorithm uses this new coordinate and the dynamic tolerance distance (DTD) to generate the secret key. This parameter and the type of movement makes this system more secure than the existing solution which depends mainly on the position of (MN) and the static tolerance distance or static location parameter.

For the implementation of this algorithm, the J2ME software is used and our proposal is tested for different locations and speeds.

Our results revealed that when the mobile phone is moving fast, the range of DTD increases which facilitate the decryption successfully with high rate. Whereas, when it moves slowly, the range of DTD decreases to reach a secure range for decryption with high successful rate. Thus, it shows the strength of our algorithm which is far stronger than static method

In the other hand, we have carried out statistical analysis, and key sensitivity analysis to demonstrate the security of the new message encryption procedure. According to the results of our security analysis, we conclude that the key is very strong Thus, it shows the strength of our algorithm and we expected to be useful for voice call encryption as future research.

5.2 Future Work

Since the ancient times, the acts of vandalism are witnessing a great demand especially on the technological devices. This has been known from acts of piracy and hackers and famous of these processes at international levels have become electronic warfare which is the language familiar to those groups. The latest trends in technological development in the world are the mobile and wireless networks which have tried too many methods of the invention and methods of sabotage.

The most dangerous types of piracy is to spy on voice calls which causes to know the characteristics of the person and everything going on around him as they represent a significant dangerous especially in the war.

In the current study, we propose to apply our idea to encrypt voice calls where it is tried to be applied in the encrypting of voice calls. But J2ME does not support this property while the OS symbian C++ has the capacity for that. Therefore, it must be to redesign the secret key from symbian C ++ language where the success of protecting the voice call by accuracy and high quality is expected.

References

[1] Ali I. Gardezi,(2006) " Security In Wireless Cellular Networks" This paper is vailable online at http://cse.wustl.edu/~jain/cse574- 06/ftp/CellularSecurity/index.html

[2] Hsien-Chou L., Yun-Hsiang C.,(2008), " A New Data Encryption Algorithm Based on the Location of Mobile Users ", Information Technology Journal, Vol. 7, No. 1,p. 63-69.

[3] Ala Al-Fuqaha , Omar Al-Ibrahim,(2007) " Geo-encryption protocol for mobile networks" ,ELESEVIER Computer Communications. No. 30, p. 2510–2517

[4] Scott,L & De Denning et al. (2003) ,"Using GPS to enhance data security GeoEncryption GPS world "

[5] V. Vijayalakshmi & Dr. T.G. Palanivelu ,(2008) " Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks ", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6

[6] Mundt ,TM (2005) "location dependent digital rights management system", In proceeding the 10th IEEE symposition on computers and communication pp: 617622

[7] Liao et al. (2007) ,"A location-dependent data encryption approach for mobile information system", in the 9th international conference on Advanced communicate technology 1:625-628

[8] P. S. Pandian, (2008) " Wireless Sensor Network for Wearable Physiological Monitoring", Journal of networks, VOL.3, NO. 5

[9] Richard Walton, (2006), " Cryptography and trust", information security technical report Vol. 11, NO. 6 8 – 7 1

[10] A. Faiz M.Maqsood,(2009). “ Information Security Threats Against Mobile Phone Services (Developer´s Perspective)”, ISSN: 1653-0187 - ISRN: LTU-PB-EX—09/046—SE

[11] http://en.wikipedia.org/wiki/History_of_cryptography

[12] http://www.it-observer.com/wireless-security-attacks-defenses.html

[13] http://www.microsoft.com/security/antivirus/bluetooth.aspx

[14] Min Song, *Old Dominion University,* (2006).”Mobile Devices and Protocols”

[15] http://kentwell.net/articles/bugbear.php

[16] Y.xiao, X.shen, D.-Z.-Du ,(2008). “Wireless Network Security”. Springer” BOOK”

[17] http://efreedom.com/Question/1-2475861/RSA-Encrypt-Decrypt-Problem-NET

[18] Introduction to cryptography and network security “book ch11”

[19] http://fr.wikipedia.org/wiki/G%C3%A9olocalisation

[20] http://www.wirelessdevnet.com/channels/lbs/features/mobilepositioning.html

[21] http:/ / www. maxmind. com/ app/ lookup_city

[22] Introduction to cryptography and network security “book ch12”

[23] Markus. Br,(2008). “Implementation of a real-time voice encryption system” master thesis

[24] Stuart. Ed, (2004) “Computer Security Strength & Risk:A Quantitative Approach” Doctor thesis

[25] Maruti. Ve, (2007). “QUASI GROUP BASED CRYPTO-SYSTEM ”Master thesis

[26] Ying. D, Tat. W et al. (2009). “ARMR: Anonymous routing protocol with multiple Routes for communications in mobile ad hoc networks” Ad Hoc Networks Elsevier B.V.VOL 7 NO 1536–1550

[27] Hwa-Chuan .L, SingLing. L, (2003). “Dynamic location strategy for hot mobile subscribers in personal communications ” Elsevier Computer Communications Vol 26 NO 1353–1364

[28] Sancho. S, Jose A. P, (2008). “Optimal switch location in mobile communication networks using hybrid genetic algorithms ” Elsevier Applied Soft Computing Vol 8 NO 1486–1497

[29] MIKKO. H, (2006). “MALLWORE MOBILE” COPYRIGHT SCIENTIFIC MERICAN, INC.

[30] Alexander. K, CSU, (2009). “Security Model Evaluation of 3G Wireless Networks ”

[31] Ratan. G, (2004). “Cryptography “

[32] Radmilo. R, Denys. M, et al., (2006). “Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone’s Battery”

[33] Shushan. Z, Akshai. A, (2007). “Building Secure User-to-user Messaging in Mobile Telecommunication Networks”

[34] Roger. K, Joachim P, et al, (2001). "Mobile Security for Internet Applications"

[35] Sowmya. Sh, Srikanth. S, et al, (2003). " Security in Mobile Computing" CS 4235A Introduction to Information Security

[36] Scott. G, Roger. K , et al, (2000). "How to Turn a GSM SIM into a Web Server" Projecting Mobile Trust onto the World Wide Web

[37] Josef. B, (2003). " Mobile Positioning for Location Dependent Services in GSM Networks" Department of Computer Science and AI, University of Malta

[38] Chris Rindal , (). "J2Me vs. .Net "Page 1 of 8 QA Technician, Tometa Software, Inc. White Paper

[39] Qijun. G, Peng. L , et al, (2004). " Hacking Techniques in Wired Networks" Pennsylvania State University, University Park

[40] Taylor Schmidt, (2009). "The History of Cryptography " Dr. Adam Harbaugh and Jenny McCarthy

[41] Stefan. S, Moritz. N, et al, (2006). " Foundations of Location Based Services" Lesson 1 CartouCHe1 - Lecture Notes on LBS, V. 1.0

[42] Michael. W, (2008). "Smart Phone Application to Influence Travel Behavior (TRAC-IT Phase 3)" FINAL REPORT (FDOT BD 549 WO 35)

[43] Andrew. O, Emmett. N. (2007). " AAMPL: Accelerometer Augmented Mobile Phone Localization"

[44] David P. Aguilar, Sean J. , et al, (2006). "Quantifying Position Accuracy of Multimodal Data from Global Positioning System–Enabled Cell Phones" Transportation Research Record 1992

[45] Amitabha. S, Pramita. M, (2004). "Next Generation Mobile Services using Location specific applications" Department Of Computer Science and Engineering Jadavpur University, Kolkata – 700032.

[46] Alex. V, MikeY. C, (2005) "Are GSM phones THE solution for localization?"

[47] Günther. R, Esmond M, (2000). "Integration of mobile phone location services into intelligent GPS vehicle navigation systems"

[48] Yang Guo, (2009). "A Mobile Distributed System for Personal Security" Department of Information Technology

[49] Manon G. Guillemette, Isabelle. F, (2008). "Hybrid RFID-GPS Real-Time Location System for Human Resources: Development, Impacts and Perspectives" vol 1530-NO 1605/08 $25.00 © 2008 IEEE

[50] MIKKO. H, (2006). “Malware Mobile” COPYRIGHT 2006 SCIENTIFIC AMERICAN, INC.

[51] http://www.cypher.com.au/crypto_history.htm

[52] http://www.tartousco.com/vb/showthread.php?3138

[53] Behrouz A. Forouzan. , (2008). “Cryptography and network security ”, McGraw-Hill Forouzen Networking Series Higher Education “BOOK”

[54] http://www.tunisia-sat.com/vb/showthread.php?t=178149

[55] http://www.reference.com/browse/cryptography

[56] http://www.businessdictionary.com/definition/cryptography.html

[57] http://searchsoftwarequality.techtarget.com/dictionary/definition/214431/

cryptography.html

[58] http://www.mobile-phones-uk.org.uk/mms.htm

[59] http://cellphones.about.com/od/phoneglossary/g/mmspicturemessaging.htm

[60] http://www.infosectoday.com/Articles/Intro_to_Cryptography/Introduction_Encryption_Algorithms.htm

[61] P.Arul, Dr.A.Shanmugam. , (2005-2009).“Generate a key for AES using biometric for VOIP network security”, Journal of Theoretical and Applied Information Technology© 2005 - 2009 JATIT. All rights reserved.

[62] B. Kaliski. “The Mathematics of the RSA Public-Key Cryptosystem “,RSA Laboratories

[63] http://en.wikipedia.org/wiki/Covariance_and_correlation

[64] H. Gao *, Y. Zhang, et al, (2006). “A new chaotic algorithm for image encryption” Chaos, Solitons and Fractals 29 (2006) 393–399 www.elsevier.com/locate/chaos

[65] http://www.zindell.com/israeliJavaBookME/ch1htm

[66] http://onjava.com/pub/a/onjava/2001/03/08/J2ME.html,

[67] http://www.esri.com/news/arcuser/0404/j2me.html

Appendix A

Hints for Existing Location Services

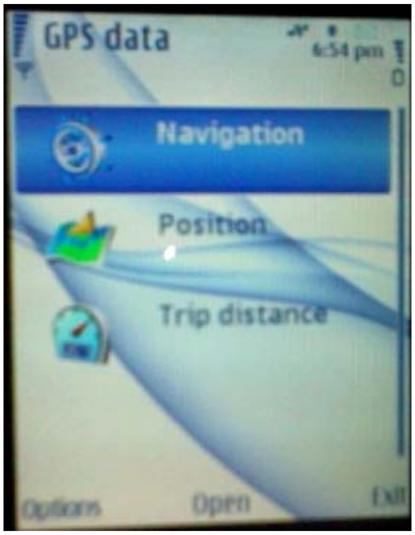
A.1 Mobile phone Location:

The location of mobile phone must be determined in real-time with two essential methods:

- Process location data in a server and deliver results to the mobile phone (FigureA-1), where the server detects location of client through the map when he gives him call.

- Read the location data directly from the application in the mobile phone (FigureA-2).

FigureA-1: Process Location Data in a Server



FigureA-2: Location Data in Device

The possibilities for location-based services/application used in mobile phone are as follow:

A.1.1 Location by GPS:

The (GPS) system in Figure (A-3) is a network of (27) satellites (including 3 emergency) turning around the Earth (2 laps in 24 hours) at an altitude of (20,200) km and over (60 sockets (4 per orbit) [42,19].

Today, most of cell phones are based of method's position which is related to (GPS) technology as in Figure (A-2).

The (GPS) uses the residual software in the mobile phone to determine the position of the device by calculating the differences between the times signals of (GPS) and satellites to reach to the receiver [42].

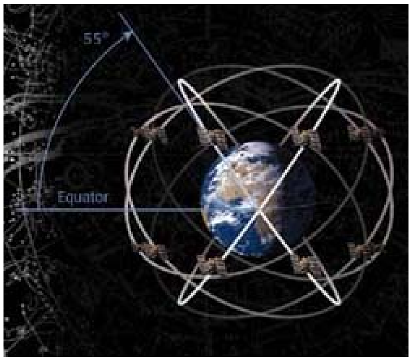
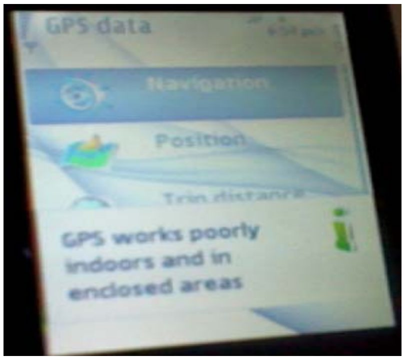


Figure A-3: GPS System



GPS works poorly indoors and in enclosed areas

Figure A-4: GPS Indoor

However, there are some drawbacks as when the mobile phone is indoor or in a clear view of the sky situations also surrounded by many tall buildings. Figure (A-4) demonstrates the (GPS) work indoor poorly.

A.1.2 Location by GSM

"Global System for Mobile Communications" (GSM) is a digital cellular phone technology which allows the positioning mobile devise based on certain information relating to (GSM) antennas to which the terminal is connected. Positioning accuracy by (GSM) can go 200 meters to several kilometers, depending on whether the terminal located in urban.

The most important type of this objective is to detect location. Several location techniques in (GSM) are mentioned as follow:

- Enhanced Observed Time Difference (E-OTD)

The (E-OTD) procedure uses the data received from surrounding base stations to measure the difference. It takes for the data to reach the terminal. That time difference is used to calculate where the user is located relative to the base stations. This requires that the base station positions are known and that the data sent from different sites is synchronized. [20].

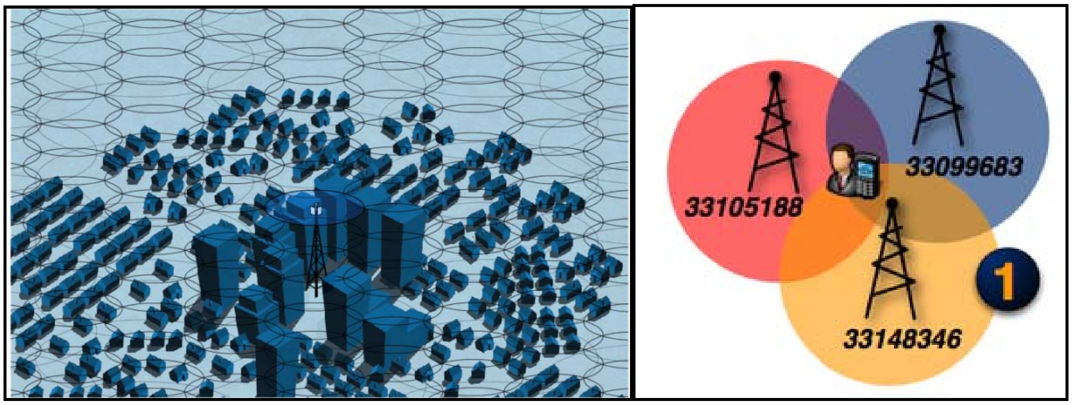
The mobile calculates the elapsed time between transmission and receipt of the request sent to the antenna. It can then calculate its distance by the following type:

- Time of Arrival

- Angle of Arrival

- Cell-ID

Today, the most used of (GSM) method is the Cell ID Figure (A-5).



(a) CELL ID'S

(b) Example of CELLID[19]

Figure A-5: Detecting location using CELL-ID

A.1.3 Location by Wireless Fidelity (WIFI)

In the same way as mobile phone can be located by the method of a Cell ID GSM network, a Wi-Fi device can use the same method based on (MAC) address detected. There are databases identifying multiple Wi-Fi access points and their location. These databases may belong to private companies or public communities which publish these databases free [19].

A.1.4 Location by IP address:

This method determines the location of a computer or any device connected to the internet based on IP address [21].

A.1.5 Location by RFID:

RFID technology can be used for indoor location. The RFID are equipped with different types of antennas which are positioned to cover the entire desired area. This technique is widely used in hospitals with low power (RFID) readers positioned in some doorways and that can tell whether a person equipped with a tag passes through [19].

A.1.6 Combination of Different Techniques:

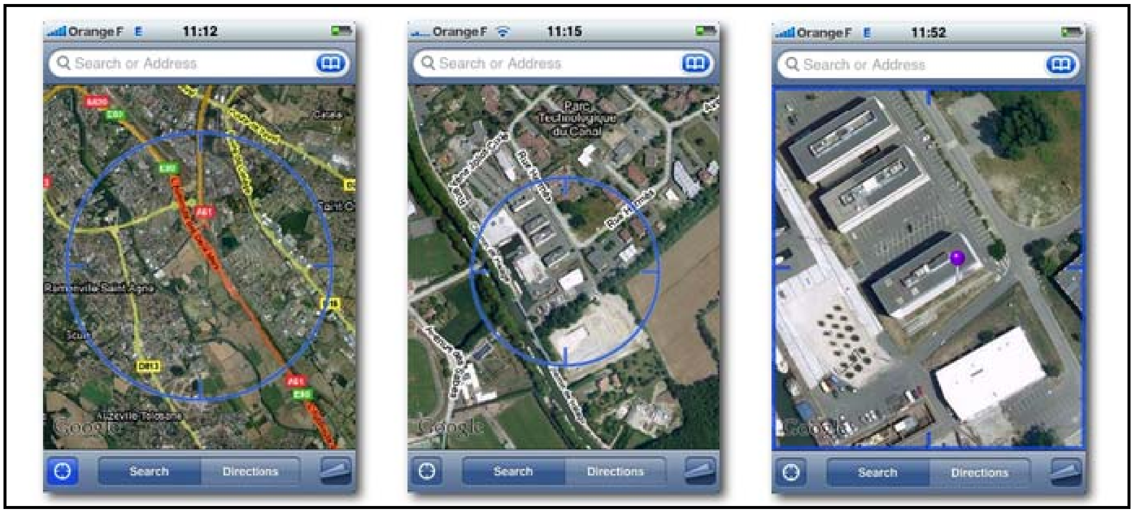
There are several drawbacks to the use of a single location:

- Dependence on GPS Network; the inability to use indoors and the response time of ignition.

- Dependence on GSM Network; geographic coverage, access to the (GPRS) network to exploit the information.

- Dependence on the presence of Wi-Fi access points: Rural example; the device that combines three techniques and being able to geo-tag the terminal in any situation exists. For example geo-tag a person outside using (GPS) and to keep track of him inside buildings or tunnels using (GSM) technology coupled with Wi-Fi for more precision.

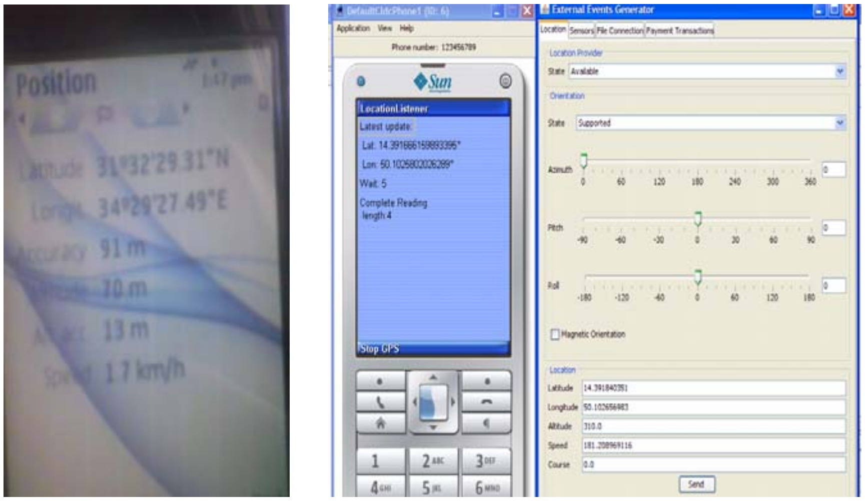
The Apple iPhone is an example of a terminal capable of using a hybrid method of geo-location interface with (GSM, Wi-Fi and GPS) receiver. This function is provided by the company skyhookwireless which provides the appropriate databases to transform identifiers cell phone and Wi-Fi access points in latitude / longitude and radius accurately. The different techniques of determining location are resumed in Figure (A-6).



(a) GSM (Cell ID) (b) GSM+WIFI (c) GPS

Figure A-6 : [19] Three different techniques of determining location.

In the j2ME software the reading of coordinate are from the GPS application installed in N6210 navigator and by J2ME emulator, as shown in Figures A-7 a,b.



```
Position
Latitude 31°32'29.31"N
Longit. 34°29'27.49"E
Accuracy 91 m
Altitude 70 m
Alt. acc. 13 m
Speed 1.7 km/h
```

```
DefaultCldcPhone1 (ID: 6)
Application View Help
Phone number: 123456789
LocationListener
Latest update:
Lat: 14.391666159893395°
Lon: 50.1025800206289°
Wait: 5
Complete Reading
length 4
Stop GPS
```

```
External Events Generator
Location | Sensors | File Connection | Payment Transactions
Location Provider
State  Available
Orientation
State  Supported
Azimuth  0
Pitch  0
Roll  0
□ Magnetic Orientation
Location
Latitude   14.391840351
Longitude  50.102656983
Altitude   310.0
Speed      181.208969116
Course     0.0
Send
```

Figure A-7: (a) Mobile phone GPS (b) Emulator GPS

Appendix B

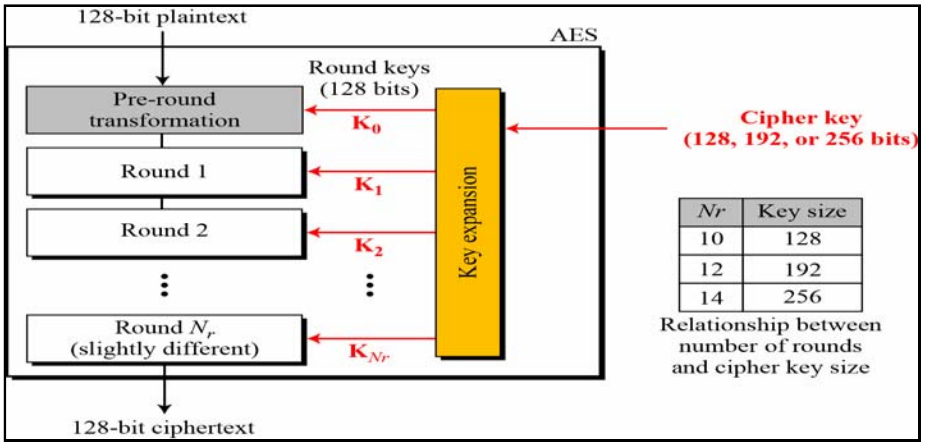
Hints from Secure Algorithm Application

B.1 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is one of the most popular algorithms used in symmetric key cryptography. (AES) is a symmetric block cipher published by the National Institute of Standards and Technology (NIST) in December 2001 which is a non-feistel cipher that can encrypt (encipher) and decrypt (decipher) data of (128) bits with variable key length and block sizes (each can be independently set to 128, 192 or 256 bits) depends on the number of rounds Figure B-1 [60, 22, 61].

(AES) is now widely used to protect classified information up to the top secret level which considered the highest security level and defined as information which would cause "exceptionally grave damage" to national security if disclosed to the public [61].

For more comprehensive surveys, the reader is referred to [22].



Nr	Key size
10	128
12	192
14	256

Figure B-1: [22] General design of AES encryption cipher

B.2 RSA Cryptosystem

The RSA [62] is public-key cryptosystem which was invented at MIT in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman[22,62].

(RSA) is the algorithm of transporting information for both encryption and authentication way through the use of pair keys, which lock or unlock a message. These keys are the private key and the public key. The public key is used to encrypt message consists of the value n which is called the modulus, and the value e which is called the public exponent. The private key is used to decrypt this message. This key consists of the modulus (n) and the value (d) which is called the private exponent.

An (RSA) [62] public-key / private-key pair can be generated by the following steps:

1. Generate a pair of large, random primes p and q.

2. Compute the modulus n as n = pq.

3. Select an odd public exponent e between 3 and n-1 that is relatively prime to p-1 and q-1.

4. Compute the private exponent d from e, p and q. (See below.)

5. Output (n, e) as the public key and (n, d) as the private key.

The encryption operation in the RSA cryptosystem is exponential to the e^{th} power modulo n:

$c = \text{ENCRYPT}(m) = m^e \bmod n$.

The input (m) is the message; the output (c) is the resulting cipher-text. In practice, the message (m) is typically some kind of appropriately formatted key to be shared. The actual message is encrypted with the shared key using a traditional encryption algorithm. This construction makes it possible to encrypt a message of any length with only one exponentiation.

The decryption operation is exponentiation to the d^{th} power modulo n: m = DECRYPT (c) = c^d mod n. (RSA) uses variable length keys, frequently 512, 1024 or 2K bits in length.

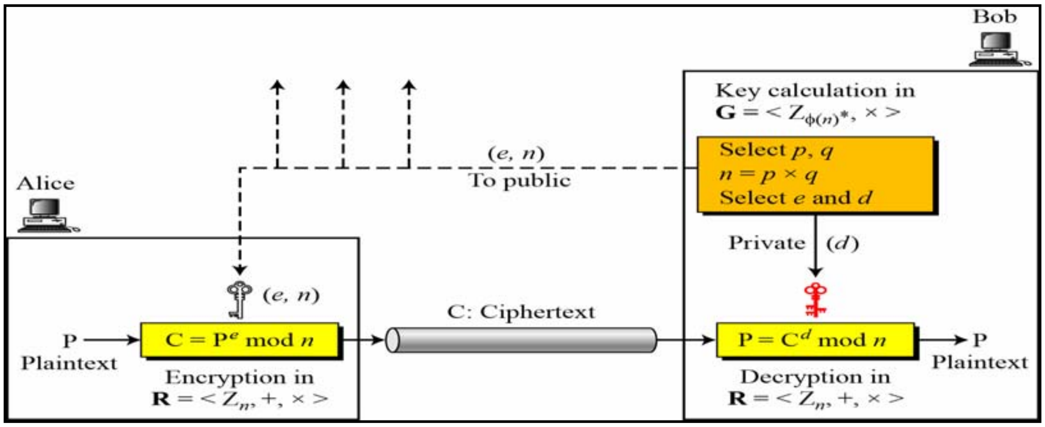


Figure B-2: [22] Encryption, decryption, and key generation in RSA

B.3 Hash Function

Hash function is a function that takes a variable length input and converts to a fixed length output, called hash value or hash digest [3]. Hash functions are relatively easy to compute but significantly harder to reverse. Beside one-way, the other important property of hash functions is collision-free: It is hard to generate two inputs with the same hash value [3,9]. The (MD5) hash algorithm is utilized as example which generates a 128-bit digest for the combined result; any hash function can applied . The hash function is used to hide the resulting value of the ellipse function which makes the secret key stronger because the result value of elliptic function is a fractional number.

Then, the digest is split into two (64-bits) values then swapped to complicate the sec-keys. This step causes that the target coordinate is unable to be derived from the sec-_key.

Appendix C

Other examples of the Experiment Results

C.1 Example of Asymmetric Algorithm (RSA)

The public key, n and e are not secure which are known to all. As n= p*q , where p and q are the large prime number. The sender chooses p and q as large prime number and calculates n= p*q . The value of $\Phi(n) = (p - 1)(q - 1)$.

Now he chooses two exponents, *e* and *d*, from $Z_{\Phi(n)}$*. he chooses *e* and d Є $Z_{\Phi(n)}$*. So, to encrypt the plain-text P, The following equation should be applied:

$C= P^e \bmod n$ to obtain the cipher-text C.

To decrypt this cipher-text we get the plain-text $P = C^d \bmod n$

Where "e, n" are the public keys and "d' is the private key

For example

The plain text:

P=14.397199304686886#14.395291138686657#50.10251610759747#50.100838502213655#0.0020930469038802357#8607f48b15a4cf8a#

means:

X_{t+1}=14.397199304686886, x_0=14.395291138686657, y_{t+1}=50.10251610759747, y_0=50.100838502213655, DTD= 0.0020930469038802357, R-key=8607f48b15a4cf8a

The cipher-text:

C=rsaenc('14.397199304686886#14.395291138686657#50.10251610759747

#50.100838502213655#0.0020930469038802357#8607f48b15a4cf8a#',pub)

```
P=char(rsadec(C,pri))
pri =    modulus: [1x308 char]

         exponent: [1x308 char]

           intent: 'private'


pub =    modulus: [1x308 char]

          exponent: '65537'

           intent: 'public'

pub.modulus

n=

169157824839652534518227444581867149706108800253795607518192831368025132
338530283898048835666165244309028028493363117160060177182734990819278271
056551115165620634206602527336603330697294693361330136936245544431269957
051381998657165795721822710226485599149735499029446311362353687129570481
921405270673338386337

>> pri.modulus

n =

169157824839652534518227444581867149706108800253795607518192831368025132
338530283898048835666165244309028028493363117160060177182734990819278271
056551115165620634206602527336603330697294693361330136936245544431269957
051381998657165795721822710226485599149735499029446311362353687129570481
921405270673338386337

>> pri.exponent

d =

944684130968961466555857679127262108311882156535837654327457410023302843
216840622956282311576918067917424636900848389163099086758335087658206008
921642860385644630072848006680846014315040432551891173607261324945851124
996228245714333801512942028518726042434208283760528261538939358165299718
409467004041210041
```

```
>> pub.exponent

e =

65537
```

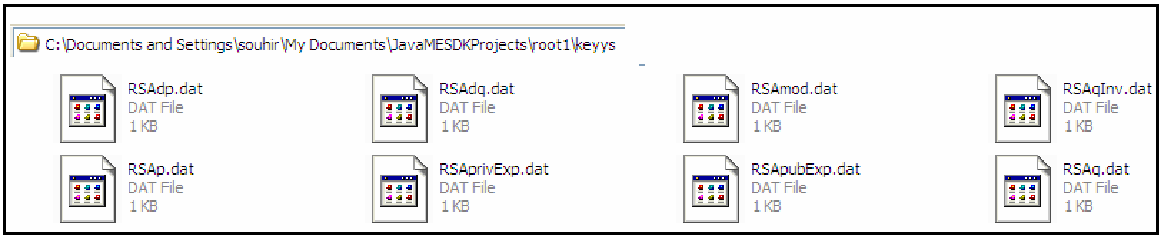
After generation of private and public key This data are saved in the RSA keys folder in figure C-3

C is the encryption data using public key applying Unit8

```
C =

  37  34  11  55  14  211  76  250  79  121  191  95  94  50  193  196  105  57  88  232  67
55
154  59  150  103  79  49  165  191  14  72  255  125  17  100  46  130  50    7  173    9  12
 15  156  241  180  255  26  150  153  170  232  178  50  206  92    8  29  242    1  195  23
9
251  39  123  240  177  102  155  113  199  91  117  185  46  115  186  184  238  91  193
22  222  183  93  36  171  210  42  64  212  213  12  90  28  156  92  15  23  143  167  160
240   24   195   69   52   207   143   68   115   66   80   208   84   19   54   50   39   71
```

P is the decryption data using private key

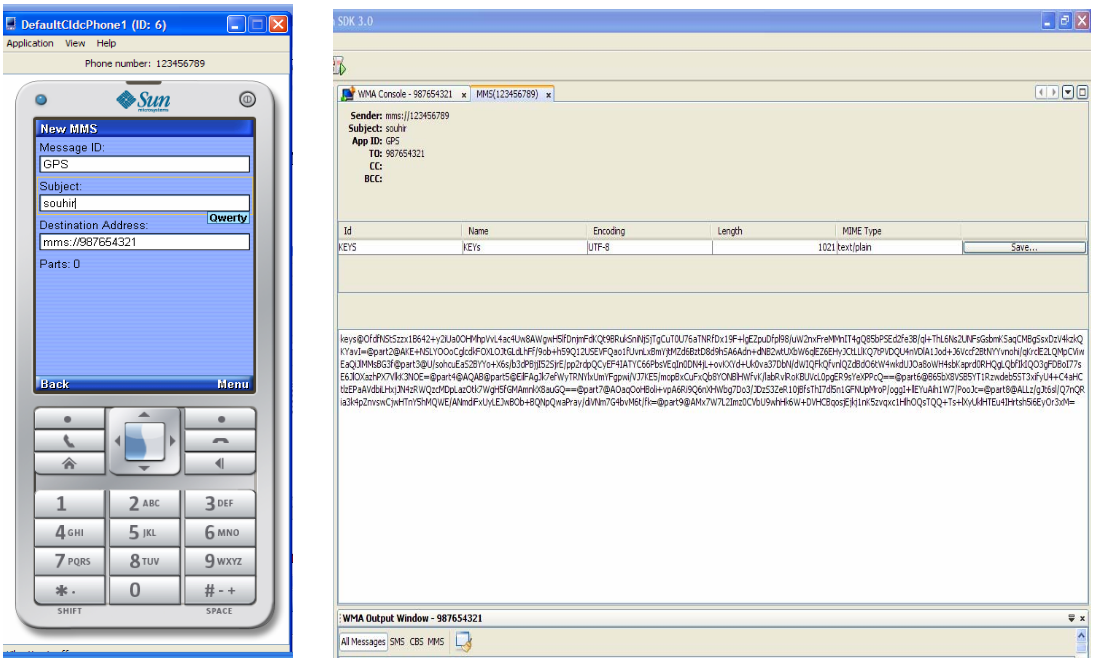
```
P =

14.397199304686886#14.395291138686657#50.10251610759747#50.100838502213655
#0.0020930469038802357#8607f48b15a4cf8a#
```



C:\Documents and Settings\souhir\My Documents\JavaMESDKProjects\root1\keyys

RSAdp.dat DAT File 1 KB	RSAdq.dat DAT File 1 KB	RSAmod.dat DAT File 1 KB	RSAqInv.dat DAT File 1 KB
RSAp.dat DAT File 1 KB	RSAprivExp.dat DAT File 1 KB	RSApubExp.dat DAT File 1 KB	RSAq.dat DAT File 1 KB

Figure C-1: RSA Keys saved in keys folder



Phone number: 123456789

New MMS
Message ID:
GPS
Subject:
souhir
Destination Address:
mms://987654321
Parts: 0

Back Menu

SDK 3.0

WMA Console - 987654321 | MMS(123456789)

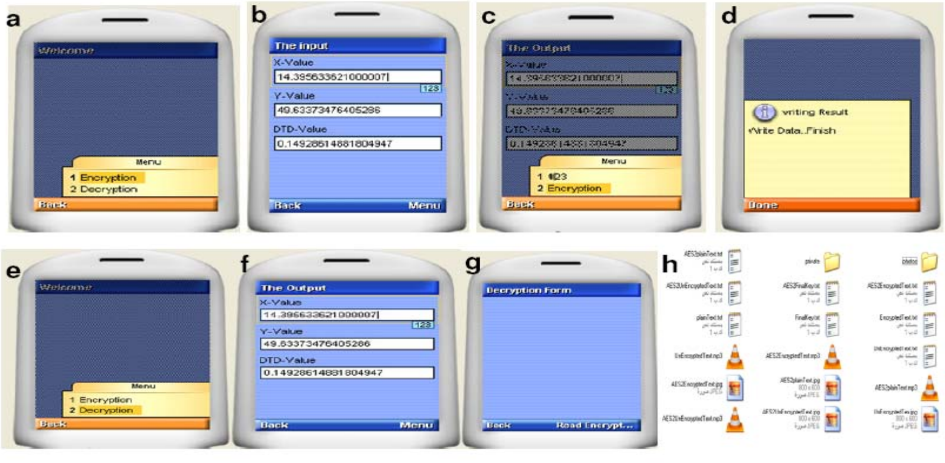
Sender: mms://123456789
Subject: souhir
App ID: GPS
TO: 987654321
CC:
BCC:

Id	Name	Encoding	Length	MIME Type	
KEYS	KEYs	UTF-8	1021	text/plain	Save...

```
keys@OfdfNStSzzx1B642+y2iUa0OHMhpVvL4ac4Uw8AWgwH5lfDnjmFdKQt9BRukSniNjSjTgCuT0U76aTNRfDx19F+lgEZpuDfpl98/uW2nxFreMMnIT4gQ85bPSEd2fe3B/ql+ThL6Ns2UNFsGsbmKSaqCMBgSsxDzV4kzkQ
KYavI=@part2@AKE+NSLYOOoCglcdkFOXLOJtGLdLhFf/9ob+h59Q12USEVFQao1fUvnLxBmYjtMZd6BztD8d9hSA6Adn+dNB2wtUXbW6qlEZ6EHyJCtLLlKQ7tPVDQU4nVDlA1Jod+J6Vccf2BtNYYvnohi/qKrclE2LQMpCViw
EaQiJlMMsBG3f@part3@U/sohcuEaS2BYYo+X6s/b3dPBjjI52SjrE/pp2rdpQCyEF4IATYC66PbsVEqIn0DN4jL+ovKXYd+Uk0va37DbN/dWIQFkQfvnlQZdBdO6tW4wkdUJOa8oWH4sbKaprd0RHQgLQbfIkIQO3gFDBoI77s
E6JlOXazhPX7VlkK3NOE=@part4@AQAB@part5@EilFAgJk7efWyTRNYlxUmYFgpwi/VJ7KE5/mopBxCuFxQb8YONBlHWfvK/labRvlRoKBUVcL0pgER9sYeXPPcQ==@part6@B65bX8VSB5YT1Rzwdeb5ST3xifyU4+C4aHC
tlzEPaAVdbiLHxjJN4zRWQzcMDpLazOtk7WgH5fGMAmnkX8auGQ==@part7@AOaqOoHBoli+vpA6Ri9Q6nXHWbg7Do3/JDzS3ZeR10jBfsThI7dl5n1GFNUpMroP/oggI+llEYuAih1W7/PooJc=@part8@ALLz/gJt6sl/Q7nQR
ia3k4pZnvswCjwHTnY5hMQWE/ANmdiFxUyLEJwBOb+BQNpQwaPray/diVNm7G4bvM6t/fk=@part9@AMx7W7L2Imz0CVbU9whHk6W+DVHCBqosjEjkj1nK5zvqxc1HlhOQsTQQ+Ts+lXyUklHTEu4IHrtsh5i6EyOr3xM=
```

Figure C-2: Generation of RSA keys converted by UTF 8 with 1021bit

C-2 Simulation Prototype



a: Welcome — Menu: 1 Encryption, 2 Decryption — Back

b: The input — X-Value: 14.395633621000007 — Y-Value: 49.63373476405286 — DTD-Value: 0.14928614881804947 — Back, Menu

c: The Output — Menu: 1 123, 2 Encryption — Back

d: writing Result — Write Data..Finish — Done

e: Welcome — Menu: 1 Encryption, 2 Decryption — Back

f: The Output — X-Value: 14.395633621000007 — Y-Value: 49.63373476405286 — DTD-Value: 0.14928614881804947 — Back, Menu

g: Decryption Form — Back, Read Encrypt...

Figure C-3 : Simulation prototype

Plain=text =

“Humanitarian Aid to Palestine Must Continue - Rosmah

KUALA LUMPUR, July 11 (Bernama) -- Humanitarian aid, including similar initiatives such as the recent Freedom Flotilla to Gaza, must continue to alert the world to the inhumane conditions in Palestine, Datin Seri Rosmah Mansor said Sunday.

The prime minister's wife said such humanitarian initiatives must be sustained and concerted to ensure it was a clear manifestation of a collective international voice which would no longer tolerate abuse, aggression and disrespect of international laws and conventions.

"In this regard, I would like to appeal to the various non-governmental organizations (NGOs) and charity organizations to continue providing humanitarian assistance to Palestine, to ensure that the much-needed assistance is made available to Palestinian territories under siege.”

Cipher-text=

“1qhF//+e7LnzLtT93+3LrMkGn1eJO4Zx7UbEtfXyEa0dC2WjHfbwkkqLnPiSa8VagrLs
pnGeLrkDxI3NsY+OfxYY2qoom6fk5xP3TCqhiSBHAQG1QpF2f0AXlhGKCGV13jfF
YxxiCm/4zSysnk1EMVzgKr49MT2fmeAm+GpiV1Jz9UTyz0EpxvkqBnbbe3vjZ/TkWt
WnXWWAsBTcXttSK5vqreHbxqKXZhkfsEBZvP2/baw0FCy9Z0YOJqyEIAa/8QYb7g
12dvEE70RdyND0vQmJE2uwwglaxLXah5OuHDt+PJjQK/4J92V/chamej4CLx8eUSvB
bxEkzv+KKw1VJ0zOtsd46F8wtCMLokHjbEGVYYTUzhY6QhEw9mu/4Y5xOpv7AT4
201b+X2u8eWzN5rh+KLefRMwQYoAH6L7BLRDjTzX3AQZmhRoTvo7d1djUgtLAX
fi9OkSdy3c/iNuBqf2vYNZ9kycy4cVDoXTdePVF3FyGxNQSlm3FbC/1EPbbwWdYQx
PZh8oVdX2sbYNsdiybwtI90EuSO6T7uoXXLF08AxwaGgYVdclZd2FRfaLMRVNXxv
T0GddocfzsUVpRHXWv0hIgiyb97K+n4Klga2IQwFqoYyZfYSE0KEh9hs95HLYY1rq/
Oqex3M5ECsRcPwCJuC2m4O3hcUPK3XaXLV+7D2g3YMnRXhyi5kyKlVunGr9qz54
Y87HawKDzwocsgFVUJgGrr/QGyou0wW8Baj38NvH3++GpyoXRFKue9lBb7c6fNN/
wTAjFyggjd2CgtQo8bxljB5cZq5r0A2ikKEmKae7h16ehYuw+29lFkBYkkoWGYeFXH
51/DUppy42laFNM2WZNTespg7Hu+RcHSILcI9LWzEtO3Ub4mu1xgArIT7HKR81Yy
r6B4mvK0Evjq8beSnALSiDuYnno7K1jhhx9bD/UQ9JoV5R0iFQC7PvO/ZGK1NZVem
DWPSGF9f+pI6Wqb1eKZYgqux8Dl+ayU1sREXnnTl0w+NrXrNhCp1R7rNWYqYZv7
g7fWYKx+8ZZTRXy2ZpriO3guoH6qBlIAhLB5PK+ExoRwjvH/ZqQI7l50PIkzoQYsQk
G0H3gFC/MbsWQWiKeXAOOqMHIkW9VJgeVQSIZ9IIZLPfee9O6MK9H”

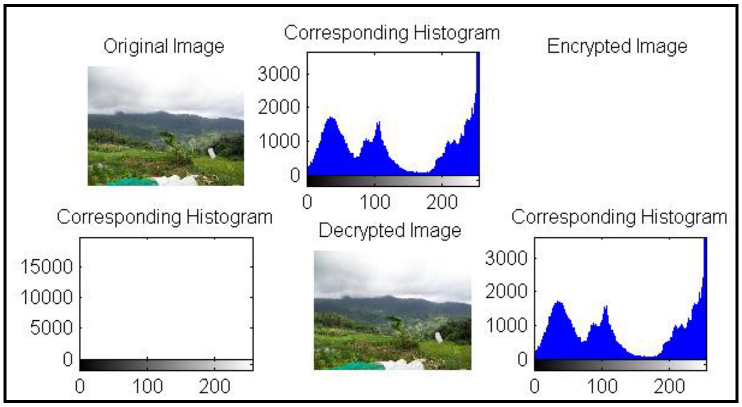
Cipher-text1=

“zKsIniC6J6p5pdu9UMIk/TmRv2eUjwFXjroa8h+zmqOlRIw2SGGSgAukpAFmJYYEv
hFiJb/7LTZpGyK9sO3b0VQpRHVbi6R/FHzHblFbZhNua4UWdQDV0hZvXwBQXg8Y
uOy4AYuQ7jvaBOESv5egDLlVmrAl2kvLMhJGCgCcrECxkwYK4VQp6O0t/YmTmx
QoMF66fUjZnie33tY8dkHPhN5x5zWWFKZb5FhMhypJrVEJ9n9xvfMVbqMLsghYQ0
YDDudJlJLJeJDYxn/uEC3ATuyy42WEVhzrW7Tnjx0kd8cKh1B70gyve+ke9Nl5CDMT
S1Hctii2K1fq1T+AbMjCUJQuaELtIQooOp9gIDumdZw1IKfZAPjgXo2lJOp0HbUURX
S2bMZwY5Wt3ING+HcDFRKyLYceo4NLu93GMbm18sNrySxlHTtK+7qp/AltO6Ek1k
sR73rAoEC5fa9uAU6OCuHoO5PrfyPZe+DrzCI8nn0Z+AeBl3Fcf9SVRPoOkWE0e7pG
SS3iLtESBfM2KI3PmUzVVVN2sH9cBSoHLQHlBv/F6+LDRqtRwx8o8f6FJiOodiQsvl
dCnSoL9odnPaQg5/0A+jqN9wkiXXED1NJU01MkFpOM2pISVMnsO7D9aNMNv7nrB
IwoHSBE/pg9IRYQFdU/2lCJDXXMO/HVYU5L0/8wzHctfgYGPHMpsMlu0xYPVUF
ELj/YySbLYJWsJxGTepSvmq+wkA7vEmtj1pFlfkEdnuY0gTYlN9QQY8VnFlErEH7F4
e2xoRyNwYgnrH+5hwQzmgclTFBih8NAcLeK/AuMCXlEqhijAs1bR6Vo97mN4hD5H
Ri8PaBekcaOzJxApz2Dgf4P8z6TtkinDHGvdg8tu1cTn9goW/EGy6BUtAatS2wsxpJavW
b2wxikUOzThzMx+58uMyCC1pMDIvQhMG4QjdZm95KpuS/2hiT8LI1C7Yfj+B21ikf
4XbizdSDozNm4abs8+rcEvC3qnYecF7GbiBMzB5fKmv9cCiwBKSeB0E+znv5pLZyTc
qgCuZDOPLsO32W2bGeHjlk9lulgPs5JrWK39yAQf1qkzdPEXMcZKFuAJWwxyEAYn
MYntCoR4xO/3zU6Ekf+iAaMwxnWF2ljI2q72nBT+fy6jW/PQfM7”

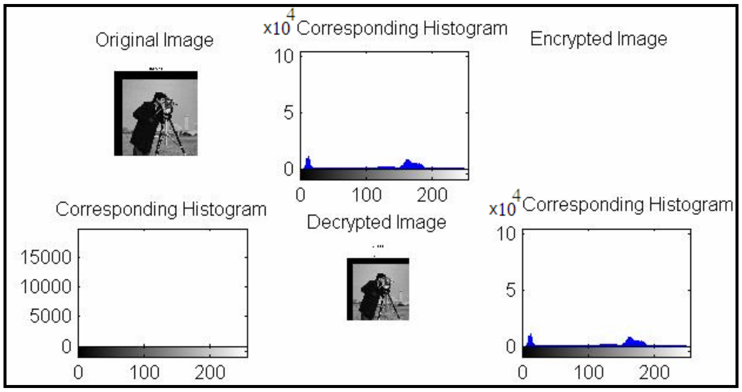
Cipher-text 2=

“BGSj3HP7Hp/A9IlD/eD6cMB+gNfXMaVPgd8VJT5JKfSGIdUDAc0hf01IOL4z6Qzn
Kc0hZ09m2icMWV90QB/FJQHjlXW6UuqiHAwb1oM84DKOk+jkolVQLb1O4JhE0tI
MOAaYUIHCdpAu3uFrtZGrPPTaCp+A5gDLWex1tFbOaaQjLnaECKsak4J3VqTZV+u
F0RaK2//pJhCRITXp5oY3ZVoCOqF4agY6yqy+6LJqF3wvaPjf+kJHpCmIPLn7gO3N2
PbVuLKS0yXhh2UDFtw8YYZUn/ffhPw1CEya+CydGS9oU9193p2rbFeuoVFcQ8huTO
M+a9wJ18mhbNhhEzaBJA3Vg/MheiMWoGOb4cf3lj32BpAK3POo5YFnZXSmJBb6K
E/CW0zn1s9/Yjd9oHeyLrgtlbrM2yutg9HLOSSTD9FBrkGpgg17YzJh3FuJDVKUw5R
NcHFSOgmq0L6rj4DpgNS9HsaiVv1+q5y/kVjwM7L1HC97u8yfl+0un9b3UURg6eDNn
rewi/wLym/pCFel0Bqfk3Ccrsvo4gyxd8PVhQg2hS3vSHLlvnblpkkfTmOCEsfn9E4rY2
GoX7tUA44bDGWnvIY+sJtT/2Gc0rAL+JGIDmy7cZxH4Wn4/wLIZnGoOeUI/C6hcJL
8LQmMAP0Tducj4SOBGHVx2X9GMD5QQQv6TBcEygyq3aAFL4DX4w1fyNZ4STi
HB88BBGN1vOzf204xyTeu86CRPUBtbaHbdTJu/e8E85md9h1XCCD285Irv4s+kY2y2
0EPX8bdgX+3NX+oQbEL5JtiySCXjrWnhbvtFYNoDBMmAst9wzpZbIUq3lGnLKshz
QPsxkFO62wyKPnM3MZPvfEQC+bH576eEO2oYTGcF8Kuo0eEibgD1tMHwXV7jeJ9
4KxWnvbTogYwuPseW0jQLDnTCLPDFRtDsJ8j73nnGWnkJOvylOVI7DbceCbq9SFy
BlKjj8Dbv7DgGBkFEsdIScRztvE7ncbi0ePqcqgPaMJ/mWmV2ROe7C4z6pM+5X0wUp
QRsASDIyZw2B3c6cSrAXyTivCqnWseo/OMV78t4+ZHkpTqXqU2f++ge8jLw4EJGCJ
yQH6elew3WQ5J7v3GOfRkNuZzYmrgBe9fkuwcMm9KlX3K7FGimhx6”

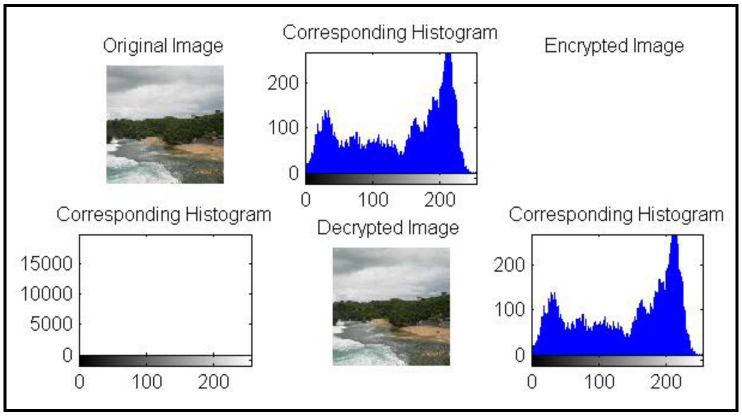
C.3 Other Examples of Histograms Result



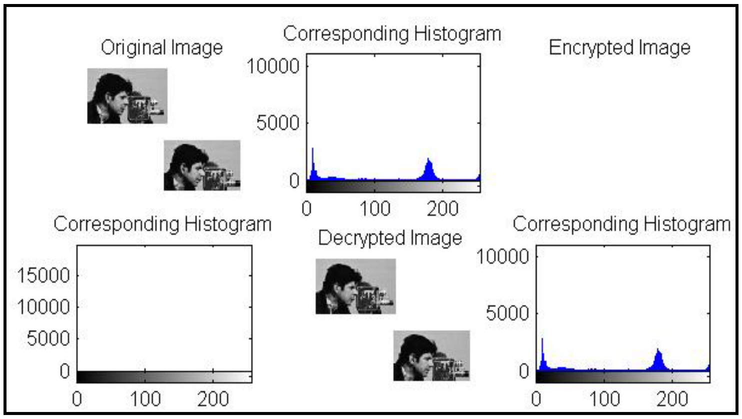
(a) Bandung image



(b) Cameraman image



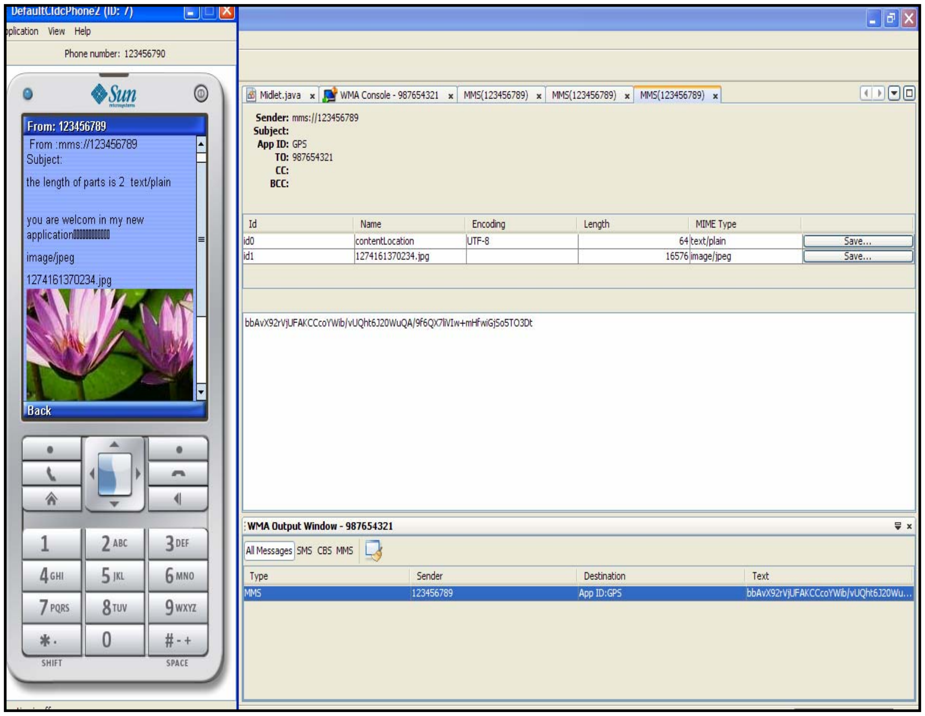
(c) krakal-beach-gunung-kidul image



(d) Oimg2 image

Figure C-4: The histogram of plain-images, cipher-images and decrypted images

C4- Other Examples of Sending/Receiving Encrypted/Decrypted MMS



Phone number: 123456790

From: 123456789

From :mms://123456789
Subject:

the length of parts is 2 text/plain

you are welcom in my new application▯▯▯▯▯▯▯▯▯▯▯▯

image/jpeg

1274161370234.jpg

Sender: mms://123456789
Subject:
App ID: GPS
TO: 987654321
CC:
BCC:

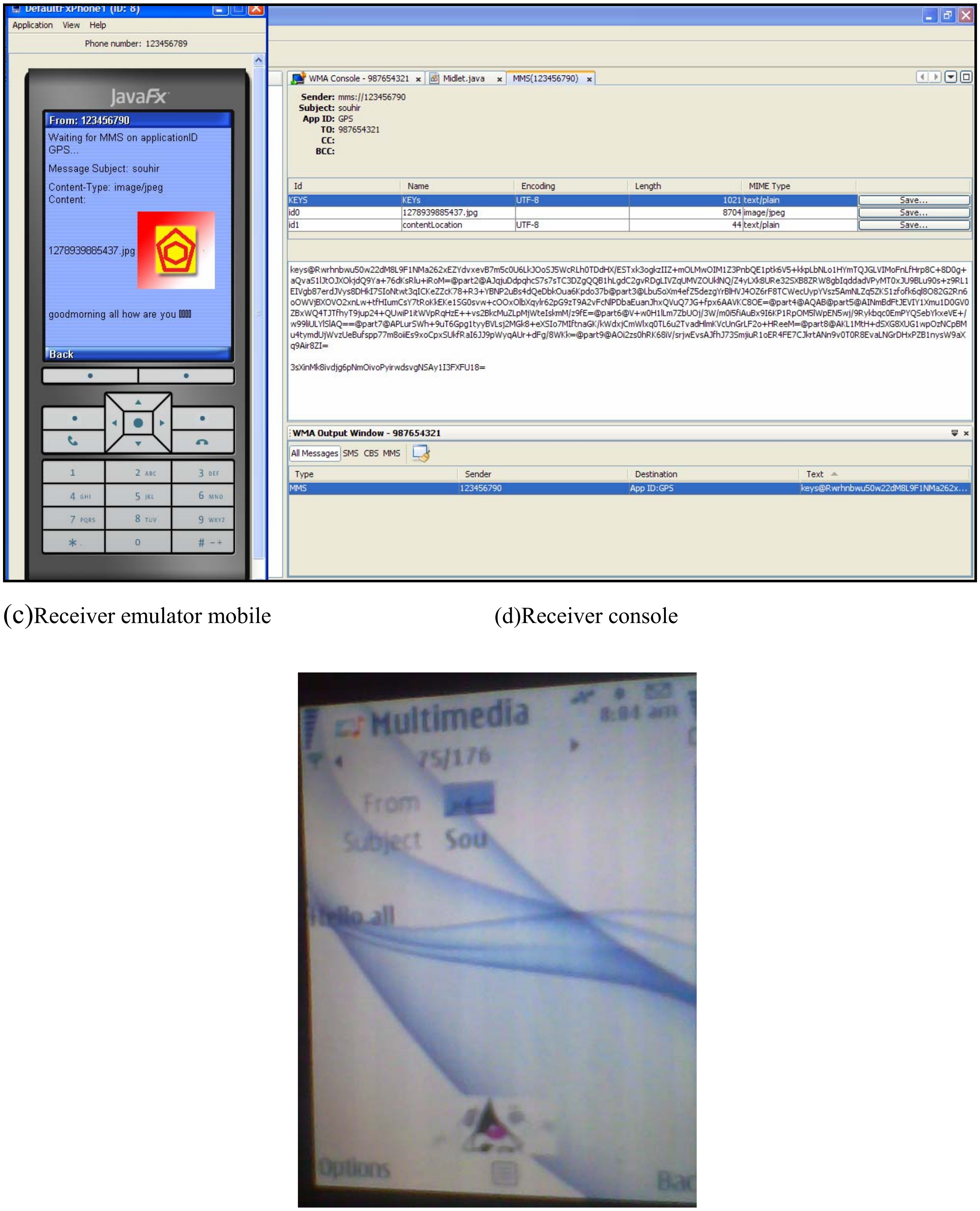
Id	Name	Encoding	Length	MIME Type	
id0	contentLocation	UTF-8	64	text/plain	Save...
id1	1274161370234.jpg		16576	image/jpeg	Save...

bbAvX92rVjUFAKCCcoYWib/vUQht6J20WuQA/9f6QX7liVIw+mHfwiGjSo5TO3Dt

Type	Sender	Destination	Text
MMS	123456789	App ID:GPS	bbAvX92rVjUFAKCCcoYWib/vUQht6J20Wu...

(a) Receiver emulator mobile (b) Receiver console

Figure C-5 (a,b) : other MMS example



DefaultFxPhone1 (ID: 8)

Application View Help

Phone number: 123456789

From: 123456790

Waiting for MMS on applicationID GPS...

Message Subject: souhir

Content-Type: image/jpeg
Content:

1278939885437.jpg

goodmorning all how are you ▯▯▯▯

Back

WMA Console - 987654321 | Midlet.java | MMS(123456790)

Sender: mms://123456790
Subject: souhir
App ID: GPS
TO: 987654321
CC:
BCC:

Id	Name	Encoding	Length	MIME Type	
KEYS	KEYs	UTF-8	1021	text/plain	Save...
id0	1278939885437.jpg		8704	image/jpeg	Save...
id1	contentLocation	UTF-8	44	text/plain	Save...

keys@Rwrhnbwu50w22dM8L9F1NMa262xEZYdvxevB7m5c0U6LkJOoSJ5WcRLh0TDdHX/ESTxk3ogkzIIZ+mOLMwOIM1Z3PnbQE1ptk6V5+kkpLbNLo1HYmTQJGLVIMoFnLfHrp8C+8D0g+
aQvaS1lJtOJXOkjdQ9Ya+76dKsRlu+iRoM=@part2@AJqjuDdpqhcS7s7sTC3DZgQQB1hLgdC2gvRDgLIVZqUMVZOUklNQ/Z4yLXk8URe32SXB8ZRW8gbIqddadVPyMT0xJU9BLu90s+z9RL1
EIVgb87erdJVys8DHkI7SIoNtwt3qICKeZZcK78+R3+YBNP2uBs4dQeDbkOua6Kpdo37b@part3@Lbu5oXm4efZ5dezgYrBlHVJ4OZ6rF8TCWecUypYVsz5AmNLZq5ZKS1zfofk6ql8O82G2Rn6
oOWVjBXOVO2xnLw+tfHIumCsY7tRoKkEKe1SG0svw+cOOxOlbXqylr62pG9zT9A2vFcNlPDbaEuanJhxQVuQ7JG+fpx6AAVKC8OE=@part4@AQAB@part5@AINmBdFtJEVIY1Xmu1D0GV0
ZBxWQ4TJTfhyT9jup24+QUwiP1itWVpRqHzE++vs2BkcMuZLpMjWteIskmM/z9fE=@part6@V+w0H1lLm7ZbUOj/3W/m0i5fiAuBx9I6KP1RpOM5lWpEN5wj/9Rykbqc0EmPYQSebYkxeVE+/
w99liULYlSlAQ==@part7@APLurSWh+9uT6Gpg1tyyBVLsj2MGk8+eXSIo7MIftnaGK/kWdxjCmWlxq0TL6u2TvadHlmKVcUnGrLF2o+HReeM=@part8@AKL1MtH+dSXG8XUG1wpOzNCpBM
u4tymdUjWvzUeBufspp77m8oiiEs9xoCpxSUkfRaI6JJ9pWyqAUr+dFg/8WKk=@part9@AOi2zs0hRK68iV/srjwEvsAJfhJ73SmjiuR1oER4FE7CJkrtANn9v0T0R8EvaLNGrDHxPZB1nysW9aX
q9Air8ZI=

3sXinMk8ivdjg6pNmOivoPyirwdsvgNSAy1I3FXFU18=

WMA Output Window - 987654321

All Messages SMS CBS MMS

Type	Sender	Destination	Text
MMS	123456790	App ID:GPS	keys@Rwrhnbwu50w22dM8L9F1NMa262x...

(c)Receiver emulator mobile (d)Receiver console

(e)Receiver real mobile in the range of DTD

Figure C-6(c,d,e): Other MMS example