

ELLIPTIC CURVES CRYPTOGRAPHY  
IN ELGAMAL CRYPTOSYSTEM

PHUA YEE BOON

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENTS FOR THE BACHELOR OF SCIENCE (HONOURS)

MATHEMATICS WITH ECONOMICS PROGRAM  
SCHOOL OF SCIENCE AND TECHNOLOGY  
UNIVERSITI MALAYSIA SABAH

APRIL 2008

PERPUSTAKAAN  
UNIVERSITI MALAYSIA SABAH



**UMS**  
UNIVERSITI MALAYSIA SABAH

## UNIVERSITI MALAYSIA SABAH

BORANG PENGESAHAN STATUS TESIS@

JUDUL: ELLIPTIC CURVES CRYPTOGRAPHY  
IN ELGAMAL CRYPTOSYSTEM.

IJAZAH: Sarjana Muda Sains Kejuruan Matematik Dengan Ekonomi

SAYA PHUA YEE BOON  
 (HURUF BESAR)

SESI PENGAJIAN: 2007/2008

mengaku membenarkan tesis (LPSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Universiti Malaysia Sabah dengan syarat-syarat kegunaan seperti berikut:-

1. Tesis adalah hakmilik Universiti Malaysia Sabah.
2. Perpustakaan Universiti Malaysia Sabah dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. Sila tandakan (/)

SULIT

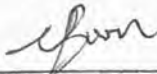
(Mengandungi maklumat yang berdarjah keselamatan atau Kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

TERHAD

(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

TIDAK TERHAD

Disahkan Oleh



(TANDATANGAN PENULIS)

(TANDATANGAN PUSTAKAWAN)

Alamat Tetap: 4-3-10, Taman  
Teratai Mewah, Jalan  
Langkawi, 53000 K.L

KHADRAB GHANIZALI

Nama Penyelia

Tarikh: 24/4/08

Tarikh: 24/4/08

CATATAN:- \*Potong yang tidak berkenaan.

\*\*Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa /organisasi berkenaan dengan menyatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT dan TERHAD.

@Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara penyelidikan atau disertai bagi pengajian secara kerja kursus dan Laporan Projek Sarjana Muda (LPSM).



## DECLARATION

I hereby declare that this dissertation contains my original research work. Sources of finding reviewed herein have been duly acknowledged.

**30 April 2007**



---

PHUA YEE BOON

HS2005-4778

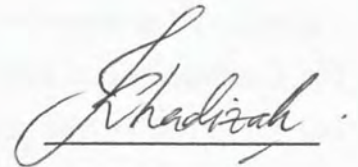


**CERTIFIED BY**

## Signatures

**1. SUPERVISOR**

(Ms. Khadizah Ghazali)

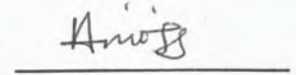
**2. CO-SUPERVISOR**

(Mr. Rajasegeran S/O Ramasamy)

---

**3. EXAMINER 1**

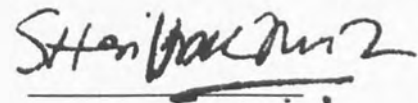
(Dr. Aini Janteng)

**4. EXAMINER 2**

(Mr. Victor Tiong Kung Ming)

**5. DEAN**

(Supt / Ks. Assoc. Prof. Dr. Shariff A.K. Omang)



## ACKNOWLEDGEMENT

First and foremost I would like to thank my supervisor and co-supervisor, Ms. Khadizah Ghazali and Mr. Rajasegeran S/O Ramasamy of the School of Science and Technology, Universiti Malaysia Sabah for their supervisions. Besides their patient guidance and generous advice, they also gave me lots of ideas in exploring field of cryptology and number theory, which are included in this dissertation.

Besides that, I would like to thank my family and friends for their supports. With their encouragement, I am more confident in doing this research.

Thank you.

Phua Yee Boon  
HS2005-4778



## ABSTRACT

This dissertation focuses on elliptic curves cryptography techniques, which is widely used in contemporary cryptography due to its promising high security with low computational overheads and speed. Fundamental number theory and theory of elliptic curves are introduced and explored. Methods and implementations of elliptic curves in cryptography techniques analogy to discrete logarithm problems has been studied rigorously. A simulation program has been written to simulate the elliptic curve version of ElGamal cryptosystem in C programming language. The program written is able to encrypt plaintext to ciphertext, and decrypt ciphertext back to plaintext.



## ABSTRAK

Disertasi ini menumpukan perhatian pada teknik kriptografi dengan menggunakan lengkung eliptik, di mana teknik ini semakin memainkan peranan penting dalam bidang kriptografi moden yang menjaminkan tahap keselamatan yang memuaskan, kos komputer yang rendah dan kelajuan pengiraan yang tinggi. Teori nombor asas dan teori lengkung eliptik dikaji. Kaedah-kaedah pelaksanaan lengkung eliptik dalam teknik kriptografi analogi kepada masalah logaritma diskrit dikaji dengan cermat. Sebuah kriptosistem ElGamal versi lengkung eliptik ditulis dalam pengaturcaraan dan simulasi C. Pengaturcaraan tersebut berjaya menukarkan teks biasa kepada teks cipher, dan seterusnya menukarkan teks cipher balik ke teks biasa.



## CONTENTS

	Page
DECLARATION	ii
CERTIFICATION	iii
ACKNOWLEDGMENT	iv
ABSTRACT	v
ABSTRAK	vi
LIST OF CONTENTS	vii
LIST OF TABLES	x
LIST OF FIGURES	xi
LIST OF SYMBOLS	xii
<b>CHAPTER 1 INTRODUCTION</b>	
1.1 Introduction	1
1.2 Cryptology	2
1.3 Secure Communications	3
1.4 Application of Cryptography	5
1.5 Study Objectives	6
1.6 Study Scopes and Limitations	7
<b>CHAPTER 2 LITERATURE REVIEW</b>	
2.1 Classical Cryptography	8
2.2 Medieval Cryptography	11
2.3 Contemporary Cryptography	13
2.4 Elliptic Curves Cryptography, ECC	17
2.4.1 Efficiencies in Elliptic Curves Cryptography	17
2.4.2 Elliptic Curves Cryptography Applications	18
2.4.2.i Application Requiring Intensive Public Key Operations	19
2.4.2.ii Applications Involving Constrained Channels	19
<b>CHAPTER 3 METHODOLOGY</b>	
3.1 Introduction	21





3.2	Groups	21
3.3	Divisor and Divisibility	23
3.4	Greatest Common Divisor, GCD	26
3.5	Extended Euclidean Algorithm	28
3.6	Modular Arithmetic or Congruences	30
3.7	The Chinese Remainder Theorem	33
3.8	Modular Exponentiation	34
3.9	Elliptic Curves	37
	3.9.1 The Group Law	40
3.10	Elliptic Curves Mod $p$	45
	3.10.1 Number of Points Mod $p$	47
	3.10.2 Discrete Logarithms on Elliptic Curves	47
3.11	Representing Plaintext in ECC	49
3.12	Singular Elliptic Curves	51
3.13	Elliptic Curves Cryptosystem	54
	3.13.1 Elliptic Curves El Gamal Cryptosystem	55
3.14	Conclusions	56
<b>CHAPTER 4 RESULTS AND DISCUSSIONS</b>		
4.1	Introduction	58
4.2	Bob's Selection of Public Key and Private Key	60
4.3	Alice's Encrypting Procedure	68
4.4	Bob's Decrypting Procedures	72
<b>CHAPTER 5 CONCLUSION</b>		
5.1	Conclusion	75
5.2	Suggestion and Future Works	76
	5.2.1 Cryptanalysis Techniques	76
	5.2.2 Elliptic Curve In Characteristic 2	77
	5.2.3 Hyperelliptic Curve Cryptography	77
	5.2.4 Primality Testing and Integer Factoring	77
	5.2.5 Stronger Computer Programming and Simulation Language	78



**REFERENCES**

79

**APPENDIX**

81



**LIST OF TABLES**

Table No.		Page
2.1	Signature Sizes On 2000 Bits Long Message.	18
2.2	Length of Ciphertext Encrypted Of 100 Bits Short Message.	18



## LIST OF FIGURES

Figure No.		Page
1.1	Secured communications.	4
2.1	Jeremiah 51:41	9
2.2	Frequencies of letters in English language.	13
3.1	$E : y^2 = x(x+1)(x-1)$ which has three real roots in two components.	38
3.2	$F : y^2 = x^3 + 73$ which has one real root in one component.	38
3.3	$P_1 + P_2 = P_3 = (x_3, y_3)$ when $x_1 \neq x_2$ .	40
3.4	$P_1 + P_2 = \infty$ when $x_1 = x_2$ .	41
3.5	$P_1 + P_2 = P_3 = (x_3, y_3)$ when $P_1 = P_2$ and $y_1, y_2 \neq 0$ .	42
3.6	$P_1 + P_2 = \infty$ when $P_1 = P_2$ and $y_1, y_2 = 0$ .	42
3.7	Singular elliptic curve $E : y^2 = x^3$ .	52
4.1	Mathematical Software Maple 10 Printscreen: Primality Testing.	62
4.2	Mathematical Software Maple 10 Printscreen: Computing Constant Coefficient For Elliptic Curve $E : y^2 \equiv x^3 + 23x + C \pmod{2579}$ .	63
4.3	Simulation Program's Printscreen (A).	64
4.4	Simulation Program's Printscreen (B)	70
4.5	Simulation Program's Printscreen (C)	71
4.6	Simulation Program's Printscreen (D)	74



## LIST OF SYMBOLS

$\mathbb{N}$	set of natural numbers
$\mathbb{Z}$	set of integers
$\mathbb{Q}$	set of rational numbers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$\mathbb{Z}/n\mathbb{Z}$	set of integers modulo $n$
$\mathbb{F}_q$	group
$\mathbb{F}_q^\times$ or $(G, \cdot)$	multiplicative group
$(G, +)$	additive group
$E/\mathbb{F}_q$	elliptic curve over group $\mathbb{F}_q$
$\mathbb{F}_{2^m}$	finite field order $2^m$
$GF(q)$	Galois Field of order $q$
*	group's operation
$\in$	element of
$a \equiv b \pmod{n}$	$a$ congruent to $b$ modulo $n$
$a   b$	$a$ dividing $b$
$a \nmid b$	$a$ not dividing $b$
$p^\alpha \parallel b$	$p^\alpha$ is the highest power of $p$ dividing $b$
$\gcd(a, b)$	greatest common divisor of $a$ and $b$
$\infty$	point of infinity in elliptic curve
$E_n(K)$	set of nonsingular points on elliptic curve $E$
$\left[ \frac{x}{K} \right]$	greatest integer less than or equal to $\frac{x}{K}$



## CHAPTER 1

### INTRODUCTION

#### 1.1 Introduction

Most of the time in our life we tried to hide something from others. Children in primary school will try to keep their examinations' marks from their friends; teenagers will find all possible ways to hide diaries away from their parents and siblings; companies absolutely do not want to see their confidential documents, secret recipes or formulae exposed to their competitors; while government will protect information of national security and military top secret by all means from non-authorized parties.

Besides keeping own information secret, at the same time human beings also curious wanted to know other's secret. Parents always try to get know what we did in our room with door closed. Boyfriend will curious what are the conversations about between his girlfriend and her pals. Ex-classmates keep asking your current salary in your school annual gathering. Bakery will want to know his competitor's secret recipe. With or without our notice, our curiosity made us wanted to know things kept secret from us.



As computer technology being developed nowadays, we sent and received information such as personal details, personal identity information, credit card or bank account numbers; we can buy almost everything, booking flight tickets or hotels, made payments with our credit cards and online banking. These are all being done in a few seconds thanks to the evolved of internet technology, World Wide Web and fibre optic broadband. However, besides the ease of online payment and banking, there come threats behind; is the important information mentioned above being transferred and remains confidential? Absolutely nobody likes this kind of important information being stolen in transactions, especially on the hand of someone with bad intentions. In many situations, we need to protect our information and keep it secret since there always someone out there will like to steal it.

The emergence of electronic cash, e-commerce and advent of internet, made cryptography techniques now applied by everyone who owns a personal computer. Computers are loaded with encryption and decryption program to protect users' data and making secured communications and transactions on the internet. Contrast to the time of our grandparents, cryptography techniques not preserve for government organizations' use in protection of government's top confidential and classified data anymore.

## **1.2 Cryptology**

Cryptology, the science of secured communication between intended users in an open channel and presence of adversaries, is derived from Greek words *kryptós* "hidden", *lógos* "word" and *ology* "science". Another word, cryptography, is always used



interchangeably with cryptology, which derived from Greek words *kryptós* “hidden” and *gráphein* “write”. Technically, cryptology is the general term for the science of secured communication and the problems in it, whereas cryptography is the process of designing and building the cryptosystem. Lastly, cryptanalysis is the study of breaking such system to extract knowledge of the information transferred. However, between cryptography and cryptanalysis, we cannot just ignore one of them. To design a good cryptosystem, knowledge of cryptanalysis is important to judge the vulnerability of newly proposed system. On the other hand, better understanding in different approaches in encryption leads us to detect weaknesses of a cryptosystem. Besides that, the science of cryptography and cryptanalysis are developed one after each other. When there is a new cryptosystem proposed to the world, somebody will find out all the ways to break it. After the cryptosystem being break by others, there will be some improvement made on it to increase its vulnerability (Lubbe, 1998).

### **1.3 Secure Communications**

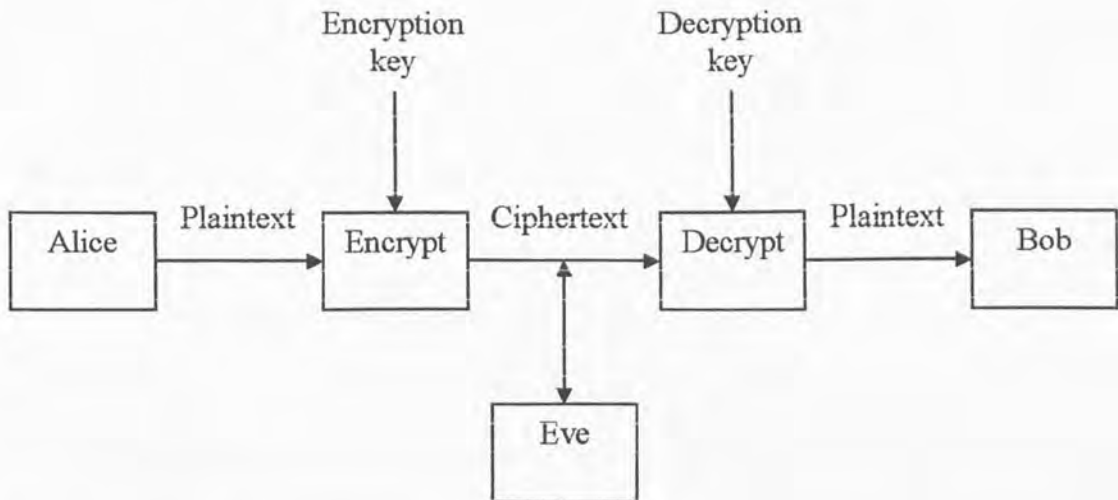
Basically, a communication described in cryptology problems involved three parties; two intended users, Alice as the sender and Bob as receiver; and adversaries represented by Eve. Sometimes the third party was given others name in some literature, which is Mallory or Oscar (Trappe, 2006). However, we will generally use the name Eve.

The original message that Alice wants to send to Bob was called plaintext. To prevent the message been able to read by adversaries when it was sent through the open channel, Alice used an algorithm and keys predetermined with Bob to scramble





the original message into disguised form; this process was known as encryption and the message in disguised form was known as ciphertext. After the cipher text reached on Bob's hand, he will change the ciphertext into plaintext using the decryption keys; this process was known as decryption (Figure 1.1).



**Figure 1.1** Secured communications

The objective of Alice and Bob is exchanging information using an open, unsecured channel but prevent Eve to get her hand on the information being exchanged. Eve's character is more complex, she can find the way to read the original message, alter Alice's message into another message before it was reached at Bob's hand, or masquerade as Alice and communicate with Bob. In the last two situations, Bob will think that the message was come from Alice (Trappe, 2006).

To get a clear picture on communication in open, unsecured channel. This can be imagined by Alice sent Bob a message using a normal postcard. Everyone who has a hand on it will get to read the message. In order to make the communication

between Alice and Bob to be secured, they now need to find a way to improve the situation. The improved situation is, for example, Alice wants to send Bob this plaintext, “i love you”. Alice scrambles the message into ciphertext that is “LORYHBRX”, wrote it on the postcard and sends it to Bob instead of the plaintext. In this situation, even though Eve can get a peek on the message on postcard being sent by Alice, she will not know what Alice wanted to tell Bob. After Bob received the postcard, he soon decrypts the ciphertext and the message is secured to only Alice and Bob.

#### **1.4 Applications of Cryptography**

Cryptography techniques used in various aspects in improving information and network security but not only encrypting and decrypting messages. There are four major applications of cryptography (Trappe, 2006).

##### **a. Confidentiality**

This is the idea to keeping intended users’ messages secret from adversaries. For example, Alice and Bob used predetermined encryption and decryption algorithms to communicate so that Eve not able to read their messages.

##### **b. Data integrity**

In communications in open network, errors may occur in the middle of transmission and thus the message maybe affected by the errors occurred. On the other hand, even though the communication is perfect without errors, adversaries are having chances to intercept the messages and alter the message before it reaches its recipients. With cryptographic primitives such as hash functions, Bob

can be more confident that the messages received has not been manipulated either by malicious or accidental adversaries.

c. Authentication

Bob wants to make sure the messages received come from Alice but not somebody else masquerade as Alice to communicate with him. There are two types of authentication in cryptography: entity authentication and data origin authentication. The term identification is always used in entity authentication which proves the identity of users in communication. Data origin authentication is about tying information of the origin of data, including sender, time and date sent etc with the data.

d. Non-repudiation

If Bob does received a message from Alice, with non-repudiation applications, Alice cannot deny she never sent such message before. In open network communication like internet, the non-repudiation is very important especially in e-commerce, which any user cannot deny the authorization of transactions or payments made by him.

## 1.5 Study Objectives

The objectives in this dissertation are:

- a. To understand classical and contemporary cryptography encryption and decryption process.
- b. To explore basic number theory which used fundamentally in contemporary cryptography technique.



- c. To find out how elliptic curves can be used in cryptography analogy to discrete logarithm problems.
- d. To implement elliptic curves in cryptography techniques based on discrete logarithm problems.
- e. To implement elliptic curves cryptography in classical ElGamal cryptosystem.
- f. To build elliptic curves version of ElGamal cryptosystem using C programming language.

## 1.6 Study Scopes and Limitations

The scopes and limitations in this dissertation are listed below:

- a. This dissertation's scope is fixed to build elliptic curve version of ElGamal cryptosystem. Hence we will concentrate solely on cryptography techniques but not cryptanalysis techniques. However, some basic idea of cryptanalysis technique was introduced.
- b. The implemented elliptic curves cryptosystem only encrypt and decrypt all characters in American Standard Code for Information Interchange ASCII but excluding the blank spaces. On the other words, we will encrypt all alphabets, numbers and symbols; furthermore alphabets are case sensitive in encrypting and decrypting process. Blank spaces should be substituted as characters underscore ' \_ ' to get correct output in encryption and decryption process.
- c. Due to the limitation of C programming in handling integers, where the largest integer for C programming to handle is 32 bits which is 4 294 967 296. We are only building cryptosystem by using prime number 2579 which is large enough to encrypt whole list of American Standard Code for Information Interchange ASCII.



## CHAPTER 2

### LITERATURE REVIEW

#### 2.1 Classical Cryptography

History of cryptography is long enough to review, almost as long as the history of written words (Bruen & Forcinito, 2005). Around four thousand years ago, there was the first known hieroglyphic symbol substitution recorded by Egyptian scribe on the stone in the tomb of Khnumhotep II, who was nobleman at that time. Even though that stone was used to praise the virtues of nobleman in stead of sending message in secret, that was the first time where substitution ciphers been used. Instead of using common symbols, that Egyptian scribe used the hieroglyphics symbol possibly only known to elite (Kahn, 1973).

In substitution ciphers, every letter in plaintext is replaced by another letter, number or symbol. For example, plaintext “crypto” may be represented as “RSPEGX” or “279786” in ciphertext. The great Roman general Julius Caesar was the first attested user who used substitution ciphers in political and military purposes. According to Suetonius, the gossip columnist of Ancient Rome, Julius Caesar encrypted messages by substitute every letter with another letter which is three places



further down when contact with Cicero and other friends. Hence, letter ‘a’ will be substituted by ‘D’, ‘b’ by ‘E’. When it comes to the end of the letters, it was wrapped around to the beginning. Then ‘x’ will be ‘A’, ‘y’ will be ‘B’ and ‘z’ will be ‘C’. Nowadays, any substitution ciphers that using shifting letters to another letter by a standard sequence like Julius Caesar is called Caesar Alphabet even if the shift is not three (Kahn, 1973).

There are at least two substitution ciphers found in Hebrew tradition Old Testament but none of them found in New Testament. One of it was found in Jeremiah 25:26, the word “SHESHACH” appear in the place where “babel” (Babylon) should be. However, the second time the word “SHESHACH” appear in Jeremiah 51:41 bring no sense of secret since the word Babylon is following immediately after its use:

“How is SHESHACH taken!”  
 “And the praise of the whole world seized!”  
 “How is Babylon become an astonishment”  
 “Among the nations!”

**Figure 2.1** Jeremiah 51:41

Another substitution is in Jeremiah 51:1, where “LEB KAMAI” (heart of my enemy) was used instead of “Kashdim” (Chaldeans). Both substitution made was called Atbash, where the first letter in Hebrew Alphabet was substituted by the last, vice versa; the second letter substituted by the second last, vice versa; and same technique applies to the rest. Which is the Hebrew equivalent of a = Z, b = Y, c = X, and so on

until  $z = A$ . In Hebrew alphabet, the second letter “b” or “beth” was replaced by the second last letter which is “SH” or “SHIN”; the letter “l” or “lamed” became “CH” or “KAPH”, which made “babel” substituted as “SHESHACH”. Similarly, the letter “kaph” in “Kashdim” changed to “LAMED” in “LEB KAMAI”. The biblical commentators were embarrassed by the words “SHESHACH” and “LEB KAMAI” in Jeremiah. They gave numerous explanations on why the secrecy is needed and even thought that “SHESHACH” is a district in Babylon. These substitutions were never meant to make message secret in communication. After all, the best explanation is the predilection of scribes to amuse them by using some word and alphabet games, bolstered by similar example from other cultures (Kahn, 1973).

Another fundamental cryptographic technique is transposition ciphers. In transposition ciphers, every letters in plaintext was rearranged or shuffled according to some predetermined formula into different position in ciphertext. For example, the plaintext of “number” will end up as “REBMUN” in ciphertext. In this case, the letters are only rearranged by reversing the original plaintext (Kahn, 1973).

The first transposition cipher was invented by the Greeks. It was recorded that the Spartans used a device named Scytale in fifth century B.C. The Scytale is a rod which wrapped spirally by strip of papyrus, leather or some writing materials made of goat or sheep skins. The plaintext which needs to be encrypted was then written on the strip, not following the direction of the strip but direction of the rod. After plaintext been written, the strip was unwrapped and the letters were found shuffled. When the receiver receive the strip, he need to have a rod that is same size with the one used by sender to read the original message (Kahn, 1973).



Besides well known with the Scytale cipher, the Greeks also transmitted message secretly in a non-cryptographic way which is known as steganography. Steganography is a method of hiding the message, which will conceal the existence of plaintext but not scrambled it as ciphertext as cryptography do (Stallings, 2003). Techniques of steganography included, character marking, invisible ink and pin punctures. The Father of History, Herodotus, revealed that how was the Greeks get important information when Persia was about to attack them. According to Herodotus, the son of Ariston, Demaratus, was an exile in Persia. When he gets knows to Xerxes's decision upon invasion of Greece. He wanted to send the information to Greece to warn the Spartans. The only way his message can be delivered securely without notice of the guards along the road was: he scraped the wax off from a pair of wooden folding tablets, write the danger message under the wood, and cover the message with wax again. After the wooden tablets reached Greece safely, Gorgo, who is Cleomenes' daughter and wife of Leonidas, discovered the secret and tell others to scrape the wax of in order to read the message underneath (Kahn, 1973).

## 2.2 Medieval Cryptography

Arabs were the first who discover and write down the methods of cryptanalysis. In 600 BCE, when Europe still in the Dark Ages, Arabs sciences, arts, medicines and mathematics flourished and became best in the world. Arabs knowledge on cryptography was published as 14 volumes encyclopedias, Subh al-a'sha in 1412. One of its authors, Qalqashandi attributed most of his information of cryptology from Ibn ad-Duraihim. Ibn ad-Duraihim held various official posts and teaching in Syria and Egypt in his life. Unfortunately, even though he was reported to authored two





## REFERENCES

- Bruen, A. A. & Forcinito, M. A. 2005. *Cryptography, Information Theory, and Error-Correction: A Handbook for The 21st Century*. Hoboken, N.J.: Wiley-Interscience, USA.
- Goldwasser, S. & Bellare, M. 2001. *Lecture Notes on Cryptography*. <http://www-cse.ucsd.edu/~mihir/papers/gb.html>
- Kahn, D. 1973. *The Codebreakers – The Story of Secret Writing*. The New American Library, Inc. New York.
- Koblitz, N. 1994. *A Course in Number Theory and Cryptography*. Springer-Verlag New York Inc., New York.
- Koblitz, N. 1998. *Algebraic Aspect of Cryptography*. Springer-Verlag Berlin Heidelberg, Berlin.
- Lubbe, J. C. A. van der (Jan C. A.). 1998. *Basic Methods of Cryptography*. Cambridge University Press, United Kingdom.
- Salomaa, Arto. 1996. *Public Key Cryptography*. Springer-Verlag Berlin Heidelberg, Berlin.
- Silverman, J. H. 2006. *A Friendly Introduction to Number Theory*. 3rd ed. Pearson Education, Inc., London.
- Smart, N. 2003. *Cryptography: An Introduction*. McGraw-Hill Education, United Kingdom.



- Stallings, W. 2003. *Cryptography and Network Security*. Pearson Education, Inc. New Jersey.
- Trappe, W. & Washington, L. C. 2006. *Introduction to Cryptography with Coding Theory*. 2nd ed. Pearson Education, Inc., London.
- Vanstone, S. A. 1997. Elliptic Curve Cryptosystem - The Answer to Strong, Fast Public-Key Cryptography for Securing Constrained Environments. *Information Security Technical Report 2* (2), pg. 78-87.
- Washington, L. C. 2003. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC, USA.
- Win, E. D. & Preneel, B. 1998. *Elliptic Curve Public Key Cryptosystem – An Introduction*. <http://www.ee.ucla.edu/~ahodjat/ECC/WWJEFCPUET8GTU83.pdf>
- Wright, M. A. 1998. The Elliptic Curve Cryptosystem: A Synopsis. *Network Security* 1998 (10), pg. 14-17.

