# ENHANCEMENT OF ENCRYPTION TECHNIQUES USING ELLIPTIC CURVE CRYPTOGRAPHY

by

**ZIAD ERSHAID AHMAD DAWAHDEH**

**( 1440211525 )**

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

**School of Computer and Communication Engineering**

**UNIVERSITI MALAYSIA PERLIS**

**2017**

**UNIVERSITI MALAYSIA PERLIS**

## DECLARATION OF THESIS

Author's Full Name : ZIAD ERSHAID AHMAD DAWAHDEH

Title : ENHANCEMENT OF ENCRYPTION TECHNIQUES USING ELLIPTIC CURVE CRYPTOGRAPHY

Date of Birth : 1 MARCH 1970

Academic Session : 2016 / 2017

I hereby declare that this thesis becomes the property of Universiti Malaysia Perlis (UniMAP) and to be placed at the library of UniMAP. This thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1997)*

☐ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

☑ **OPEN ACCESS** I agree that my thesis to be published as online open access (Full Text)

I, the author, give permission to reproduce this thesis in whole or in part for the purpose of research or academic exchange only (except during the period of _____ years, if so requested above)

Certified by:

| | |
|---|---|
| **SIGNATURE** | **SIGNATURE OF SUPERVISOR** |
| O047751 | DR. SHAHRUL NIZAM BIN YAAKOB |
| **(NEW IC NO. /PASSPORT NO.)** | **NAME OF SUPERVISOR** |
| Date: 12 October 2017 | Date: 12 October 2017 |



**NOTES** : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with the period and reasons for confidentiality or restriction. Replace thesis with dissertation (MSc by Mixed Mode) or with report (coursework)

## ACKNOWLEDGMENT

First of all, my great thanks are truly to Our God who has helped me and gave me the strength and patience to complete this work. I would like also to express my heartfelt gratitude to my supervisor Dr. Shahrul Nizam Yaakob for his help, cooperation, advice, guidance, and for all those hours of enjoyable discussions which helped me to complete my thesis work. His valuable and constructive suggestions at many difficult points of the thesis work are highly acknowledged. Also, I want to thank my co-supervisor Dr. Rozmie Razif bin Othman for his encouragement and help during my study. My sincere obligation goes to the Dean of the Computer and Communication Engineering School in the UniMAP University and all the staffs of the school for their support and help that they give to the students during their studies.

My wholehearted thanks to my father for his support, encouragement, and prayer to me for success during all periods of my life. Also, I would like to give great thanks to my family; my lovely wife, my sons, and daughter for their support, motivations, and patience on living far from them during my study. Also, I would like to thank my brothers and sisters for their encouragements.

Finally, I dedicate this work to the spirit of my beloved mother, may God have mercy on her.



Ziad Ershaid Dawahdeh

School of Computer and Communication Engineering

University Malaysia Perlis (UniMAP)

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ASCII | American Standard Code for Information Interchange |
| DES | Data Encryption Standard |
| DLP | Discrete Logarithm Problem |
| EC | Elliptic Curve |
| ECC | Elliptic Curve Cryptography |
| ECCHC | Elliptic Curve Cryptography with Hill Cipher |
| ECDLP | Elliptic Curve Discrete Logarithmic Problem |
| EGECC | ElGamal Elliptic Curve Cryptosystem |
| $E(F_p)$ | The set of all points on an elliptic curve E defined over $F_p$ |
| $E_p(a,b)$ | Elliptic group over the Galois Field |
| GF($p$) | Galois Field (The finite field of order $p$, where $p$ is prime) |
| MEGECC | Modification of ElGamal Elliptic Curve Cryptosystem |
| MMVECC | Modification of Menezes-Vanstone Elliptic Curve Cryptosystem |
| Mod($m$, $p$) | Remainder of dividing $m$ by $p$ |
| MSE | Mean Squared Error |
| MVECC | Menezes-Vanstone Elliptic Curve Cryptosystem |
| NPCR | Number of Pixels Change Rate |
| $Ord(G)$ | The order of the point $G$ |
| PDA | Personal Digital Assistant |
| PSNR | Peak Signal to Noise Ratio |
| RSA | Rivest, Shamir and Adleman |
| UACI | Unified Average Changing Intensity |

## LIST OF SYMBOLS

| | |
|---|---|
| $A$ | Addition |
| $\equiv$ | Congruent |
| $D$ | Doubling |
| $P, Q, R$ | Elliptic Curve points |
| $\in$ | Element of |
| $E$ | Elliptic curve |
| $F_p$ | Finite prime field |
| $G$ | Generator point (Base point) |
| $I$ | Identity matrix |
| $M$ | Message |
| *mod p* | Modulo *p* |
| $\#E$ | Number of points on $E$ |
| $O$ | Point at infinity |
| $p$ | Prime number |
| $K$ | Secret key |
| $K_m$ | Self-invertible key matrix |
| $\Sigma$ | Summation |

**Peningkatan Keupayaan Teknik Enkripsi Dengan Menggunakan Kriptografik Elliptik Melengkung**

## ABSTRAK

Proses enkripsi dan penyahsulitan mengambil lebih banyak masa bagi melaksanakan proses pengiraan matematik. Matlamat utama kerja penyelidikan ini adalah untuk meningkatkan keupayaan teknik enkripsi ElGamal, Menezes-Vanstone, dan Cip Cipher dengan menggunakan Cryptography Curve Elliptic bagi mempercepat pengiraan MEGECC dan MMVECC, serta meningkatkan tahap keselamatan dan kecekapan ECCHC. Dalam MEGECC yang diubahsuai, ia menggunakan kod ASCII heksadesimal dan bukan kod ASCII perpuluhan dimana ia dapat mengurangkan bilangan dua kali ganda serta menambah operasi dalam pendaraban skalar dan melonjakkan pengiraan matematik. Hanya operasi penambahan serta penolakan yang digunakan dalam MMVECC yang dicadangkan, dan tiada operasi penyongsangan atau pendaraban yang digunakan kerana ia menggunakan masa yang lebih lama berbanding penambahan dan penolakan, selain menggunakan kod ASCII hexadecimal untuk mempercepat pengiraan. Pengubahsuaian ketiga dalam kerja penyelidikan ini diterapkan pada algoritma Hill Cipher asal, dimana ia mempunyai struktur yang mudah dan pantas, tetapi dari segi keselamatan adalah lemah. Pendekatan penyulitan hibrid baru antara Elliptic Curve Cryptosystem dan asal Hill Cipher yang dicadangkan bagi menukar Hill Cipher dari teknik simetri menjadi satu asimetris dan meningkatkan keberkesanan keselamatannya. Matriks utama boleh terbalik digunakan untuk menghasilkan kunci rahsia penyulitan dan penyahsulitan. Keupayaan untuk menyulitkan setiap watak dalam jadual ASCII 128 dengan menggunakan nilai ASCII perpuluhan secara langsung tanpa jadual pemetaan adalah sumbangan lain dalam pendekatan ECCHC. Kesemua tiga pengubahsuaian dalam tesis ini digunakan pada mesej teks dengan saiz yang berbeza dan saiz skala kelabu yang berlainan. Untuk pesanan teks, bilangan tambahan dan operasi dua kali ganda dan juga masa penyulitan / penyahsulitan yang diperlukan dalam teknik yang dicadangkan telah dikira dan dibandingkan dengan teknik lain. Analisis Histogram, Analisis Entropi, Nisbah Puncak kepada Noise Noise (PSNR), Unified Average Changing Intensity (UACI), dan Number of Pixels Change Rate (NPCR) telah digunakan untuk menilai kecekapan enkripsi gambar skala kelabu dan menilai prestasi teknik enkripsi yang dicadangkan. Keputusan pada mesej teks menunjukkan bahawa teknik tersebut adalah lebih cepat daripada teknik lain. Bagi imej skala kelabu, keputusan untuk MEGECC, MMVECC, dan ECCHC menunjukkan bahawa purata nilai entropi adalah 7.9895, 7.9856 dan 7.9921 masing-masing, yang sangat hampir kepada nilai maksimumnya 8, serta purata nilai PSNR adalah 8.8771, 8.8642 , dan 8.7661 yang sangat rendah, juga peratusan purata bagi NPCR adalah 99.9932, 100, dan 100 yang sama atau sangat hampir kepada nilai ideal 100. Hasil simulasi ini menunjukkan bahawa teknik yang dicadangkan dapat meningkatkan kecekapan teknik yang ada; mengurangkan bilangan pendaraban skalar, meningkatkan kecekapan dalam pengiraan matematik, meningkatkan keselamatan dan kecekapan bagi menentang ancaman penggodam.

**Enhancement Of Encryption Techniques Using Elliptic Curve Cryptography**

## ABSTRACT

Encryption and decryption processes consume more time for mathematical calculations. The main goal of this research work is to improve ElGamal, Menezes-Vanstone, and Hill Cipher encryption techniques by using Elliptic Curve Cryptography to speed up the calculations in MEGECC and MMVECC, and increase the security level and key efficiency in ECCHC. In the modified MEGECC, using hexadecimal ASCII code instead of decimal ASCII code reduced the number of doubling and adding operations in the scalar multiplications and sped up the mathematical computations. Only addition and subtraction operations are used in the proposed MMVECC, and no inversion or multiplication operations are used because it consumes a longer time compared to addition and subtraction, besides using hexadecimal ASCII code to speed up calculations. The third modification in this research work is applied on the original Hill Cipher algorithm, it has a simple structure and fast computations, but weak security. A new hybrid encryption approach between Elliptic Curve Cryptosystem and original Hill Cipher has been proposed to convert Hill Cipher from symmetric technique to asymmetric one and increase its security effectiveness. Self-invertible key matrix is used to generate encryption and decryption secret key. The ability to encrypt every character in the 128 ASCII table by using its decimal ASCII value directly without a mapping table is another contribution in ECCHC approach. All the three modifications in this thesis are applied on text messages of different sizes and different grayscale images of size $256 \times 256$. For text messages, the number of addition and doubling operations and also the encryption/decryption time needed in the proposed techniques are calculated and compared with other techniques. Histogram Analysis, Entropy Analysis, Peak Signal to Noise Ratio (PSNR), Unified Average Changing Intensity (UACI), and Number of Pixels Change Rate (NPCR) have been used to assess the grayscale image encryption efficiency and evaluate the performance of the proposed encryption techniques. The results on the text messages show that the proposed techniques in this study are faster than other techniques. For grayscale images, the results for MEGECC, MMVECC, and ECCHC show that the average of the entropy values are 7.9895, 7.9856, and 7.9921 respectively, which are very closed to the theoretical value 8, and the average of PSNR values are 8.8771, 8.8642, and 8.7661 which are very low, also the average of NPCR percentages are 99.9932, 100, and 100 which are equal or very closed to the ideal value 100. These results indicate that the proposed techniques improved the efficiency of the existing techniques; reduced the number of scalar multiplications, sped up the mathematical calculations, increased the security and efficiency, and resisted the adversaries.

# CHAPTER 1: INTRODUCTION

## 1.1 Background

Data exchange is rapidly increased recently by the increasing use of the internet and communications media. Sharing information, such as Text, Image, Audio, and Video over unsecured channels is liable for attacking and stealing. Cryptography is one of the mathematical techniques that ensure secure communications within a non-secure channel and protect information from adversaries and increase the security of communications. Encryption is needed to convert plaintext (original data) to ciphertext (unreadable) before sending it via the internet to the other user (recipient). Decryption is done by the receiver to return the ciphertext back to the original data. Symmetric (private key) and asymmetric (public key) encryption techniques are two groups of cryptography. In symmetric encryption, the same key (private key) is used for encryption and decryption processes, whereas in asymmetric encryption the sender uses a private key differ than the receiver's private key and each party generates the public and secret key separately after agreeing on elliptic curve domain parameters (Hankerson, et al., 2004; Bokhari & Shallal, 2016).



Elliptic Curve Cryptography (ECC) is one of the most effective techniques that are used for information security. It depends on the hardness of the elliptic curve discrete logarithm problem (ECDLP). So, the adversaries are not able to attack ECC and solve ECDLP which is infeasible to be solved and has strong security against all kinds of attacks (Sagheer, 2012; Wenger & Wolfger, 2014). Also, ECC provides a smaller key size compared to other systems like RSA, where a key size of 160 bits in ECC is equivalent to that accorded by 1024 bits in RSA (Alese, et al., 2012; Rajadurga &

Kumar, 2014; Gupta, et al., 2015; Magons, 2016). Elliptic Curve (EC) has been introduced and used for the first time in cryptography separately by Miller (1985) and Koblitz (1987). ECC can be defined over two types of fields: one is the prime field $F_p$ which is suitable for the software applications and the other is the binary field which is suitable for the hardware applications (Stallings, 2011). ECC has some advantages that make it widely used recently such as small storage capacity, faster computations, and reduction of the power consumption (Gutub, et al., 2007; Minfeng & Wei, 2010; Gutub & Khan, 2011; Rabah, 2016). These benefits make ECC more suitable to be used in smart cards, wireless communications, PDAs, portable devices, and e-commerce applications (Gupta & Silakari, 2011; Gaithuru, et al., 2015; Rabah, 2016).



### 1.2 Problem Statement

Encryption and decryption processes in ElGamal Elliptic Curve Cryptosystem (EGECC) and Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC) consume more time for the scalar multiplication computations (Hongqiang, et al., 2013; Wang, et al., 2014; Ruma & Hailiza, 2014; Mirghadri & Rahimi, 2015). Therefore, speed up the calculations of encryption and decryption processes and reduce the time consumed in computations in these techniques is one of the aims of this research.

The Hill Cipher algorithm is one of the symmetric techniques; it has high throughput, high speed, and simple structure, but weak security because both sender and receiver should use and share the same key (private key) via unsecured channels (Acharya, et al., 2009; Agrawal & Gera, 2014; Mahmoud & Chefranov, 2014; Ramesh, 2015). So, the second aim of this research is to increase Hill Cipher security effectiveness by proposing a new hybrid encryption approach between Elliptic Curve

Cryptosystem and Hill Cipher (ECCHC) to convert Hill Cipher from symmetric technique (private key) to asymmetric one (public key) and make it resists the hackers.

### 1.3 Objectives of the Study

The main goal of this research is to enhance the efficiency of the proposed encryption techniques (ElGamal, Menezes-Vanstone, and Hill Cipher) and increase its security level and speed up the calculations by improving the use of Elliptic Curve Cryptography over prime fields. It uses hexadecimal ASCII values instead of decimal ASCII values for every character in the 128 ASCII table and reduces the number of scalar multiplications needed with encryption and decryption processes. The main objectives of this study are:

1. To reduce the number of scalar multiplications needed with encryption and decryption processes and speed up the computations in the proposed ElGamal ECC and Menezes-Vanstone ECC techniques.
2. To increase the security effectiveness for the proposed Hill Cipher algorithm.



### 1.4 Scope of the Study

The scope of the study is as follows:

1. The research is limited to enhance (ElGamal, Menezes-Vanstone, and Hill Cipher) encryption techniques using ECC over prime fields.
2. Planning, development, implementation, testing, and analysis of all related processes of the encryption techniques.

3. The proposed techniques will be implemented for all characters and symbols in the 128 ASCII table and grayscale images of size $256 \times 256$ using MATLAB R2013a (8.1.0.604) 32-bit software on Core i5 computer with CPU 2.53 GHz and RAM 4 GB.

## 1.5 Significance of the Study

The enhancements that have been proposed in this study will increase the efficiency and security of the encryption techniques and make it more resistant for the adversaries. It will also speed up the computations and reduce the time consumed for it, and increase the complexity of the calculations by using hexadecimal ASCII values. These advantages make the cryptography techniques suitable to be used in smart cards, wireless communications, PDAs, portable devices, and e-commerce applications (Gupta & Silakari, 2011; Rajadurga & Kumar, 2014; Rabah, 2016).



## 1.6 Contributions of the Study

The enhancements that will be done in this study will increase the efficiency of the encryption techniques and make it more suitable to be used in smart cards and small devices and applications. The main contributions of this research are:

1. To enhance ElGamal ECC algorithm by using hexadecimal ASCII value instead of decimal ASCII value to transform each character in the plaintext message into two affine points on the elliptic curve over a finite prime field which increases the complexity of the encryption technique. Also, speeds up the mathematical

computations by reducing the number of addition and doubling operations needed in scalar multiplication operations.

2. To improve Menezes-Vanstone ECC algorithm by using a new and simple structure mathematical equations for encryption and decryption processes that depends on addition and subtraction only and no need to compute the inverse operation in the decryption process because it consumed a long time. Besides using hexadecimal ASCII values for the characters in the plaintext instead of decimal ASCII values which increases the complexity of the encryption technique for the adversaries.
3. To develop the novel approach ECCHC that combines ECC with the original Hill Cipher to produce a new public key (asymmetric) technique that has a high level of security and resists the adversaries because no need to share the secret key over unsecured channels and the new secret key depends on the discrete logarithm problem (DLP) which is very hard to be solved by the attackers.



## 1.7 Thesis Structure

This thesis shall be organized into five chapters. Chapter 1 provides an introduction to the work, problem statement, the objectives, the scopes of this research, and explains the significances and contributions of this study.

Chapter 2 contains an overview of the main concepts of encryption and decryption. The main two types of encryption; symmetric and asymmetric, and the differences between them are also discussed. The main operations that are related to the Elliptic Curve function are introduced in this chapter. A brief description of the original algorithms: ElGamal ECC, Menezes-Vanstone ECC, Diffie-Hellman technique, and original Hill

Cipher and the previous studies related to the proposed techniques are also introduced. A description of the main security measures that evaluate the efficiency of the cryptography techniques on grayscale images is also explained.

Chapter 3 presents and discusses in details the methodology that will be applied to enhance the security level of the encryption and decryption processes by using the new proposed approaches. A description of the new modifications in the proposed techniques is also given in details.

Chapter 4 discusses the implementation, testing, and results analysis of the proposed techniques by using different examples of text messages and grayscale images of size $256 \times 256$. A comparison between the results obtained by the proposed techniques and the results of other related techniques are also shown.

Chapter 5 summarizes the main conclusions of the research work and the recommendations for the future work.

# CHAPTER 2: LITERATURE REVIEW

## 2.1 Introduction

This chapter gives the basic mathematical concepts for elliptic curve function over the prime finite field used in this study to modify the proposed cryptography systems. A detailed description of the original encryption techniques used in this study and a review of some related previous contributions in this area are also provided. The rest of this chapter is arranged as follows: Section 2.2 gives a brief history of cryptography. Section 2.3 introduces an overview of the two categories of cryptography systems: symmetric and asymmetric key cryptography. An overview of ECC and its importance is described in Section 2.4. Section 2.5 gives a mathematical description of the main arithmetic operations on EC over a prime field. A brief description of Elliptic Curve Discrete Logarithm Problem (ECDLP) is given in Section 2.6. Section 2.7 provides a description of the cryptography techniques: ElGamal ECC, Menezes-Vanstone ECC, Diffie-Hellman, and original Hill Cipher and a review of the previous related works of each technique. Section 2.8 describes the main methods used to assess the proposed techniques on text messages. An explanation of the most important image security measures is given in Section 2.9. Finally, Section 2.10 summarizes this chapter.



## 2.2 History of Cryptography

Cryptography is the art of hiding information and prevent unauthorized access and keep data secure from the adversaries. Cryptography return back to 4000 years. The Chinese used it to hide words meaning in their messages. Secret codes were used in the

Indian government communications. Replacing the last letter of the alphabet by the first one was another ciphering technique used by the Babylon and Asyria. Julius Ceasar used another cryptography technique by shifting each letter in the plaintext 2 places through the alphabet and replacing it with another letter. This method was called substitution cipher because it substituted each letter in the plaintext by another letter to form the encrypted message (Cohen, 2001).

In 1795, Thomas Jefferson invented the wheel cipher which consisted of a set of wheels, each with a random ordering of the letters of the alphabet, and the key of the encryption is the ordering of the wheels on the axle (Cohen, 2001). In 1917, the cryptographic organization MI-8 was established by the Americans. They analyzed encryption messages, codes, and secret inks. In 1929, Lester S. Hill invented a new cryptography technique that assigned a numerical value for each plaintext letter and ciphered it by using matrices multiplication. In 1948, Shannon invented one of the modern cryptography techniques based on mathematical computations. Shannon developed 'Unicity Distance' which is a method to measure the cryptography technique's strength and used to break any ciphered message (Cohen, 2001).



Data Encryption Standard (DES) was one of the strong cryptography techniques, it published by the US government and widespread because it's based on mathematical operations (Davies, 1997). Asymmetric (public key) cryptography was used for the first time by Whitfield Diffie and Martin Hellman in 1976, it represents the modern encryption techniques that uses two types of keys; one called private key and the other called public key (Davies, 1997).

In 1978, Rivest, Shamir, and Adleman published their new algorithm RSA, which used exponentiation modulo in encryption and decryption. It was one of the first

techniques that used public key cryptography. Its security depends on the difficulty of factoring two large prime integers (Calderbank, 2007; Stallings, 2011).

In 1985, Miller and Koblitz independently introduced and used Elliptic Curve (EC) which is a new public key cryptographic system. Elliptic curve cryptography (ECC) depends on the hardness of the elliptic curve discrete logarithm problem (ECDLP). So, the adversaries are not able to attack ECC and solve ECDLP. For this reason, most of the modern cryptographic systems are established based on the EC (Hankerson, et al., 2004; Sagheer, 2012).



### 2.3 Symmetric and Asymmetric Cryptography

Cryptography is one of the mathematical techniques that is used to protect information (Text, Image, Audio, and Video) from adversaries and increase the security of communications. Encryption is needed to convert plaintext (original data) to ciphertext (unreadable) before sending it via the internet to the other user (recipient). Decryption is done by the receiver to return the ciphertext back to the original data. The security of encrypted data is dependent on the strength of the cryptographic algorithm and the secrecy of the key. Symmetric (private key) and asymmetric (public key) encryption techniques are two groups of cryptography (Stallings, 2011). Ganpati & Tyagi (2015) performed a study shows that Asymmetric key cryptography is more secure and efficient than Symmetric key cryptography.

In symmetric encryption, the same key (private key) is used for encryption and decryption processes. It uses transposition (transposes the position of the characters in the plaintext to another position) and substitution (maps the characters of the plaintext