UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

TEXT ENCRYPTION USING ELLIPRIC CURVE CRYPTOGRAPHY (ECC) OVER BINARY FINITE FIELD AND ELGAMAL CRYPTOSYSTEM

P40S19

AHMAD ASIF BAKHTIAR NOOR BIN NOOR HAMID (2017976503)
NOR SYAZWANI BINTI NOR ZAILAN (2017371965)
SYAZA FARLISA BINTI ISHAK (2017996399)

Report submitted in partial fulfilment of the requirement
for the degree of
Bachelor of Science (Hons.) Computational Mathematics
Faculty of Computer and Mathematical Sciences

DECEMBER 2019

ACKNOWLEDGEMENTS

IN THE NAME OF ALLAH, THE MOST GRACIOUS, THE MOST MERCIFUL

Firstly, we are grateful to Allah S.W.T for giving us the strength to complete this project successfully.

We would like to express our greatest gratitude to our supervisor, Miss Nur Lina Binti Abdullah for always give us continuous knowledge and support to complete our study. Without her help to assist us to understand all our problems in our study, we might face more problems in completing this study. Next, we would like to thank to all our group members that had always been dedicated and always gave their full commitment in order to make our study successful no matter how hard it was. Each of our member give their best to share their opinion and knowledge to obtain the result of this study successfully. We are also grateful for having a very supportive family that always give their best support throughout our journey in completing our study. Other than that, we also would like to thank all our lecturer and our class members who have always being supportive towards each other and always help us technically and mentally throughout our journey in completing this study.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS i

TABLE OF CONTENTS ii

LIST OF TABLES iii

ABSTRACT iv

1. INTRODUCTION 1

1.1 Problem Statement 3

1.2 Objective 3

1.3 Significance of Study 3

1.4 Scope of Study 4

2. LITERATURE REVIEW 5

2.1 Background Theory 5

2.1.2 Basic Number Theory 5

2.1.2 Cryptography 7

2.2 Literature Review 13

3. METHODOLOGY AND IMPLEMENTATION 15

3.1 The Proposed System 17

3.2 Numerical Example 20

4. RESULTS AND DISCUSSION 27

4.1 Result 27

4.2 Discussion 27

5. CONCLUSIONS AND RECOMMENDATIONS 29

REFERENCES 30

LIST OF TABLES

Table 1: 16 Elements of $\mathbb{F}_{2^4}$ 20

Table 2: Value for all power of g 21

Table 3: All point on the elliptic curve $y^2 + xy = x^3 + ax^2 + b$ with $a = g^4$ and $b = 1$ 21

Table 4: List of alphanumeric characters 23

Table 5: The differences between numbers of keys appearing in the system 28

LIST OF FIGURE

Figure 1: Proposed System 20

ABSTRACT

Cryptography consists of some algorithms but the most common algorithms that had been used are Elliptic Curve Cryptography (ECC) and Rivest-Shamir-Adleman (RSA). ECC use very small keys, it is a way to be more effective computationally and makes it ideal for the smaller and less powerful devices that most people use to access network services. Due to small keys that had been offered by ECC, instead of RSA, ECC had been used widely in practical applications in embedded system such as mobile devices and IC card. finite field. ECC can be perform by using either finite field or binary field. Text encryption using ECC over binary finite field, $Gf(2^m)$ has more advantage than finite field, $Gf(p)$ but the previous study that use ECC and ElGamal for text encryption only represent the system using $Gf(p)$. We observed that to implement Elgamal cryptosystem in binary finite field, there are a few modification that need to be done to satisfy the properties of binary finite field. This is to ensure that the message that had been send can be decrypt successfully. The algorithm that will be used in this paper to complete the encryption and decryption process is ElGamal algorithm. Motivated from Natanael & Suryani in 2018, we represent the finite field using binary finite field $Gf(2^m)$ or $\mathbb{F}_{2^m}$. Therefore, in this study, the implementation of ECC over $\mathbb{F}_{2^m}$ with the modification of ElGamal encryption and decryption scheme work successfully where the original message or plaintext had been obtained after decryption process. For future studies, this method can be further improves by using a larger value of m in $\mathbb{F}_{2^m}$ in order to increase the security of the text message. This method also can be implemented in GUI to make the calculation of encryption and decryption process faster instead of calculating manually.