

UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

**IMPLEMENTING ELLIPTIC CURVE CRYPTOGRAPHY ON
COMMUNICATION KEY IN ELLIPTIC CURVE INTEGRATED
ENCRYPTION SCHEME**

MUHAMMAD HAZIQ BIN MOHD JEFRY (2019257322)

MUMTAZATUN NISA' BINTI AIDIL FIZZA (2019291046)

NAF'AN BIN NASHA (2019218992)

(P9M22)

**Report submitted in partial fulfillment of the requirement
for the degree of**

Bachelor of Science (Hons.) (Computational Mathematics)

Faculty of Computer and Mathematical Sciences

AUGUST 2022

ACKNOWLEDGEMENTS

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

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

First and foremost, we would like to thank Allah SWT, the most gracious and the most merciful, for granting us the strength and ability to complete this project. Without His permission, we would not be able to successfully complete this project.

We would also like to convey our gratitude to our supervisor, Encik Md Nizam bin Udin, for his guidance and time spent throughout the process of completing this project from day one until it is successfully done.

Apart from that, we would also want to thank Dr Zati Aqmar Binti Zaharudin for her help, advice and courage to complete the proposal for this project. Not to forget, Dr Nur Azlina Abd Aziz, our final year project lecturer who has been following up with our group project progress to make sure we are on track. Besides that, she also gives advice and corrects our mistakes in writing this report.

Last but not least, we would like to thank our beloved family for the motivation and understanding given to us throughout the process of completing this project.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	i
TABLE OF CONTENTS	ii
LIST OF FIGURES	iii
LIST OF TABLES	iii
ABSTRACT	iv
CHAPTER 1: INTRODUCTION.....	1
1.1 Background of the study	1
1.2 Problem Statement	4
1.3 Objectives	4
1.4 Significant and Benefit of Study.....	4
1.5 Scope and Limitation of Study.....	4
1.6 Definition of Terms and Abbreviations	5
CHAPTER 2: BACKGROUND THEORY AND LITERATURE REVIEW	7
2.1 DHKE	7
2.2 ECDH.....	8
2.3 ECIES	8
CHAPTER 3: METHODOLOGY AND IMPLEMENTATION.....	10
3.1 Research Framework	10
3.2 Elliptic Curve Modulo a Prime	11
3.3 Addition Law of Elliptic Curve	12
3.4 ECIES	13
CHAPTER 4: RESULTS AND DISCUSSION	18
4.1 Finding points on Elliptic Curve.....	18
3.2 Modified ECIES Protocol.....	22
4.3 Implementation of the Proposed Algorithm	24
CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS.....	27
5.1 Conclusion	27
5.2 Recommendation	27
REFERENCES.....	28

LIST OF FIGURES

Figure 1: Flowchart of the research framework.....	10
Figure 2: Elliptic Curve	12
Figure 3: Four ways of a line interception on elliptic curve	12
Figure 4: Flowchart of ECIES protocol	14
Figure 5: The proposed algorithm.....	22

LIST OF TABLES

Table 1: Definition of terms and abbreviation	5
Table 2: Quadratic residue of 17.....	18
Table 3: Finding points on elliptic curve	20
Table 4: Point addition on elliptic curve.....	21

ABSTRACT

In today's modern world, most data transactions and communications are made through online channel. However, exchanging data over an insecure channel is harmful since malicious actors would use the data to their benefits. Therefore, to ensure the security when making data transmission online, cryptography was introduced. Security and efficiency of cryptosystem depends on the mathematical problem that it is based on. Despite that, when a cryptosystem has been created for quite a long time, the cryptosystem might have been broken by hacker. Hence, it is important for cryptographer to develop a more secure and advanced cryptosystem. In this project, we will be examining the current state of knowledge about Diffie-Hellman Key Exchange (DHKE) protocol and Elliptic Curve Diffie-Hellman (ECDH), modifying communication keys from numbers to point based on Elliptic Curve Cryptography (ECC) and changing the method of establishment of communication keys from multiplication law to addition law. With the new method that we have proposed, we hope that it can benefit academicians for future research and can be implemented in real world.