UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

MESSAGE EMBEDDING TECHNIQUE IN ELLIPTIC CURVE CRYPTOGRAPHY USING MULTIPLE OF POINTS

P9M19

NUR SYAFAWANI BINTI MAT SYET	2017696456
UMMI AFIFAH BINTI MOHAMAD ARSAD	2016718503
MUHAMMAD FAIZ BIN ABDUL SHUKOR	2016534961

Report submitted in partial fulfillment of the requirement
For
Bachelor of Science (Hons.) Mathematics
Faculty of Computer and Mathematics Sciences

JULY 2019

ACKNOWLEDMENT

IN NAME OF ALLAH, THE MOST GRACIOUS, THE MOST MERCIFUL. Firstly, Alhamdulillah. We are grateful to Allah S.W.T for His Faithfulness and giving us the opportunity to finish this Final Year Project successfully.

The deepest appreciation to our supervisor, Md Nizam Bin Udin who guides us for two semesters to completes this project by giving the continued support, the consultation also the guidelines for this project. Without his encouragement, it is hard for us to finish this project perfectly.

Special thanks also to those people who directly or indirectly helped in the project. Their help that consists of sharing idea and information helps us a lot to build up the perfection in this project.

Last but not least, thanks for our parent that always support us in a various way. They are the people that give us an inspiration and build our spirit to complete this project.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

Public key cryptosystem is a famous technique that has been developed by using elliptic curve. In this paper, a method of embedding plaintexts is proposed in binary field, $GF(2^5)$; it is irreducible polynomial and satisfies condition $b \neq 0$. Maple 2016.1 is used to show how the encryption and decryption works. Thus, a method is implementing into MVECC protocol successfully based on encryption and decryption.