UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

MODIFICATION OF TEXT ENCRYPTION BASED ON ELLIPTIC CURVE CRYPTOGRAPHY (ECC) AND CAYLEY-PURSER ALGORITHM

P20M19

NURUL SAKINAH BINTI ISMAIL (2016299092)

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

JULY 2019

ACKNOWLEDGEMENTS

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

Alhamdulillah, all praises to Allah for the strengths and His blessing for giving me a chance in completing this project.

Special thanks and appreciation goes to my supervisor, Miss Nur Lina binti Abdullah, for her supervision and constant support along my ongoing project. Her valuable help of constructive comments and suggestions throughout the ongoing project have contributed to the success of this study. Not forgotten, thanks to my Cryptography lecturer, Mr. Md Nizam bin Udin for providing guidance to me and classmates regarding about the Cryptography lesson. His teachings in Cryptography subject which linked to my study gave a deep learning for me to understand and self-studied throughout this semester. I learnt new things outside the class and think out of the box to complete the mathematical algorithm. Furthermore, I sincerely thanks to all my lecturers, friends and others for their continuous support whenever I felt down and about to give up. Last but not least, my deepest gratitude goes to my beloved parents; Mr. Ismail bin Samah and Mrs. Julaila binti Mohlas and also to my siblings for their endless love, prayers and encouragement

TABLE OF CONTENTS

ABSTRACT

The modified scheme is considered secure against eavesdroppers if the suitable points on the elliptic curve are remains hard to be found. However, even this problem remains hard today, it is still very likely in the future that efficient algorithms are found and the ECC problem could be solving. Therefore, one of the strategy to surmount this situation is by designing a scheme with multiple hard problems. Motivated from that, this study reviewed the arithmetical properties of elliptic curve and Cayley purser algorithm. After studying the arithmetical properties, this study propose to modify Kamalakannan-Tamilsevans's scheme (2015) by adding double layers of encryption and decryption. The theoretical aspects of this scheme are analyzed, concluding that the modified scheme have successfully work very well.