UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

MODIFICATION OF BLOM'S KEY PRE-DISTRIBUTION SCHEME BY USING ELLIPTIC CURVE

P17S19

SITI AISHAH BINTI MOHD RIDZUWAN (2017953171)
NUR ANNISA BINTI ZULKIFILI (2017971821)
NUR ATIQAH BINTI GHAZALI (2017148457)

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

DECEMBER 2019

ACKNOWLEDGEMENTS

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

Alhamdulillah, firstly, we are very grateful to Allah S.W.T. for giving us the strength and health to complete the project successfully.

We would like to express our biggest gratitude and sincere appreciation to our Final Year Project`s supervisor, Sir Md. Nizam Bin Udin for all the assistance, guidance, and feedbacks to help us improve the quality of this project. Without his assistance, we would not be able to complete this project well.

Not forgetting Prof. Madya Nur Azlina Binti Abd Aziz and Dr. Nor Azni Binti Shahari, the lecturers who have also provided with various kinds of advice, support and encouragement throughout the whole process of completing this report. Their contributions are deeply appreciated by the members of this study for without them, we will not be able to complete this report successfully.

Last but not least, we would like to thank our parents and fellow colleagues who have been very supportive, thoughtful and cooperative in sharing the information and knowledge that they possess. Their kind thoughts and actions inspire us deeply.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Symmetric cryptography uses a unique key for both encryption and decryption. There is an issue that rose regarding the key transaction which might be interrupted by an unauthorized party and it costs a high price. Thus, key pre-distribution scheme is created in order to overcome the mentioned issue. One of the protocols is Blom`s Key Pre-distribution scheme. However, Blom`s Key Pre-distribution scheme uses integer finite field which makes this scheme to be easy to be intervened by attackers. Hence, this project suggests a different appeal by implementing elliptic curve into the Blom`s Key Pre-distribution scheme to overcome the disadvantages since the security of elliptic curve is better than the prime number being used in the original scheme. As a result, the overall process of the modification of Blom`s Key Pre-distribution scheme techniques is presented and demonstrated through a Graphical User Interface (GUI). The future researches of this same study should consider applying some of the protocols in Elliptic Curve Cryptography (ECC) and run a few tests on the scheme to ensure the performance of the modified scheme.