

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

	PAGE
1. ACKNOWLEDGEMENTS	i
2. TABLE OF CONTENTS	ii
3. LIST OF FIGURES	iii
4. LIST OF TABLES	iii
5. ABSTRACT	1
6. 1.0 INTRODUCTION	2
1.1 INTRODUCTION	2
1.2 PROBLEM STATEMENT	4
1.3 OBJECTIVES OF THE STUDY	4
1.4 SCOPE AND LIMITATIONS OF THE STUDY	4
1.5 SIGNIFICANCES OF THE STUDY	5
7. 2.0 BACKGROUND THEORY AND LITERATURE REVIEW	6
2.1 BACKGROUND THEORY	6
2.2 LITERATURE REVIEW	11
8. 3.0 METHODOLOGY	14
PHASE 1: IDENTIFY SCHEMES TO BE USED	15
PHASE 2: MODIFICATION BLOM'S KEY PRE-DISTRIBUTION SCHEME	17
PHASE 3: DEVELOPMENT OF GRAPHICAL USER INTERFACE (GUI)	21
9. 4.0 RESULTS AND DISCUSSION	23
4.1 RESULTS	23
4.2 IMPLEMENTATION OF THE STUDY	29
10. 5.0 CONCLUSIONS AND RECOMMENDATIONS	31
11. 6.0 REFERENCES	32
12. APPENDIX	35

LIST OF FIGURES

	PAGE
1. Figure 1: Geometric Proof of Point Addition in Elliptic Curve	7
2. Figure 2: Geometric Proof of Point Doubling in Elliptic Curve	8
3. Figure 3: Blom's Key Pre-distribution Scheme	9
4. Figure 4: Flowchart of the Research Study	14
5. Figure 5: Modification Blom's Key Pre-distribution Scheme	17
6. Figure 6: Flowchart of the Process of Graphical User Interface	21
7. Figure 7: Graphical User Interface (GUI) of the Proposed Scheme	30
8. Figure 8: Example of Graphical User Interface of Proposed Scheme with Inserted Values	39

LIST OF TABLES

	PAGE
1. Table 1: The Points on the Elliptic Curve	23
2. Table 2: The Figuring Points on $K_{A,B}$ and $K_{B,A}$	28
3. Table 3: Steps to Utilize the Graphical User Interface	29

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.