UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

IMPLEMENTATION OF SCHNORR DIGITAL SIGNATURE INTO BLOM'S KEY PREDISTRIBUTION SCHEME

NUR ADDAMERA AFIEQA BINTI MOHD AZRI	**2020878634**
FATIMAH AZZAHRAA BINTI ABDUL GHANI	**2020819238**
NUR AMNI NATASYA BINTI ROSLAN	**2020621566**

P10M23

Report submitted in partial fulfillment of the requirement
for the degree of
Bachelor of Science (Hons.) (Mathematics)
College of Computing, Informatics and Media

AUGUST 2023

ACKNOWLEDGEMENTS

IN THE NAME OF ALLAH, THE MOST GRACIOUS, THE MOST MERCIFUL. All praises to Allah and His blessings for the completion of this report. We thank Him for all opportunities, trials, and strength that have been showered on us to finish this report. We experienced so much during the making of this report, not only from an academic aspect but also from the aspect of personality to do it. Our humblest gratitude to the holy Prophet Muhammad (Peace be upon him) whose way of life has continuously guided us.

First and foremost, we are grateful to Allah S.W.T. for giving us the strength to complete this project successfully. Thank you also goes out to our parents as well as friends who were constantly encouraging us throughout the process when we felt discouraged or became frustrated because they knew how much work went into this venture.

We would like to express our gratitude to Sir Md Nizam bin Udin our supervisor, for giving us a good guideline for the report throughout numerous consultations. We would also like to expand our deepest gratitude to all those who have directly and indirectly guided us in completing this assignment.

Last but not least, many thanks go to all teammates of the project, who have invested their full effort in managing the team in achieving the goal. We also have to appreciate the guidance given by our classmates in our project report, it has improved our skills thanks to their comments and advice.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS ii
TABLE OF CONTENTS iii
LIST OF FIGURES iv
LIST OF TABLES iv
ABSTRACT v
CHAPTER 1: INTRODUCTION 6
1.1 Motivation 6
1.2 Problem Statement 8
1.3 Objectives 8
1.4 Significant of Study 9
1.5 Scope and Limitation of Study 9
1.6 Definition of Terms 9
CHAPTER 2: BACKGROUND THEORY AND LITERATURE REVIEW 12
2.1 Background Theory 12
2.2 Literature Review/ Related Research 12
2.2.1 Cryptography 12
2.2.2 Blom’s Key Predistribution Scheme 13
2.2.3 Schnorr Digital Signature 15
CHAPTER 3: METHODOLOGY AND IMPLEMENTATION 17
3.1 Schnorr Digital Signature 17
3.2 Blom’s Key Pre-distribution Scheme 22
3.3 Proposed Method: Modification of Blom’s Key Predistribution Scheme by Implementing Schnorr Digital Signature. 26
CHAPTER 4: RESULTS AND DISCUSSION 27
4.1 Modification of Blom’s Key Predistribution Scheme 27
4.2 The computation proposed method by using Maple Software 2016. 33
4.3 The Comparison of the Proposed Scheme with Other Existing Schemes 34
CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS 35
REFERENCES 36
APPENDIX 40

LIST OF FIGURES

Figure 1: Schnorr Digital Signature…………………………………………………..17
Figure 2: Blom's Key Predistribution…………………………………………………...22
Figure 3: Modification of the Proposed Method……………………………………...26
Figure 4: Modification of Blom's Key Predistribution Scheme………………………...27

LIST OF TABLES

Table 1: Comparison of the proposed scheme with other existing schemes……………..34

ABSTRACT

In symmetric cryptography, the encryption and decryption processes each employ a different key. There is a problem with the important transaction that has come up that might be expensive and interrupted by an unauthorised person. Therefore, a key predistribution scheme is created in order to overcome the mentioned issue. Blom's key predistribution scheme is one of the protocols. Blom's key predistribution scheme, uses an integer finite field, making it easy for attackers and criminal activists to intervene. Hence, this study suggests implementing the Schnorr Digital Signature to enhance the security of the original Blom’s. In this proposed method, points generated through the Schnorr Digital Signature will be designed as public identifiers to be used in the original scheme. Each user's private key and session key are generated using the addition of law mathematical process with allocated public identifiers. A shared session key will be obtained by n^{th} users who intend to communicate with each other. As a result, this study will present the overall process of the modification of Blom’s key predistribution scheme. Furthermore, it has been proved that the modified scheme can generate a common session key share between three users such as $K_{AB} = K_{BA} = K_{BC}$ to be used in the encryption and decryption processes. In the future, this method can be improved by using the signing and encryption method also known as signcryption that was proposed by (Zheng, 1997). This method can be used for secure and authenticated message delivery which fulfills both the functions of digital signature and encryption with a cost significantly lower and less in computation time.