UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

IMPLEMENTING MULTI PRIME RSA DIGITAL SIGNATURE IN SHAMIR'S THREE PASS PROTOCOL

MUHAMMAD ARIF MUSA BIN ABDULLAH - 2020976723

MUHAMMAD ALIF HAIDHAR BIN HALIM - 2020943777

NUR MUHAMMAD DANISH BIN RAISHAM – 2020371469

P61S22

Report submitted in partial fulfilment of the requirement

for the degree of

Bachelor of Science (Hons.) (Mathematics)

Mathematical Sciences Studies

College of Computing, Informatics and Media

FEBRUARY 2023

ACKNOWLEDGEMENTS

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

Firstly, I am grateful to Allah S.W.T for giving me the strength to complete this project successfully.

we would like to thank to extend my sincere toward all personages who have helped us in this endeavour. Without their active guidance, help, cooperation, and encouragement, we would not have made headway in this project.

We are ineffably indebted to Mr. Nizam bin Udin for his conscientious guidance and encouragement to accomplish this assignment.

We extend our gratitude to Universiti Teknologi MARA (UITM) for giving us this opportunity. After that, we also acknowledge with a deep sense of reverence, our family members, who always supported us morally as well as economically.

Finally, our gratitude goes to all our friends who directly or indirectly help us to complete this project report.

Thank you.

ACKNOWLEDGEMENTS ..... **ii**
LIST OF FIGURES ..... **iv**
ABSTRACT ..... **v**
CHAPTER 1: INTRODUCTION **1**
1.1 Motivation 1
1.2 Problem Statement 4
1.3 Objectives 5
1.4 Scope and Limitation of Study 5
CHAPTER 2: LITERATURE REVIEW **6**
2.1 Introduction 6
2.2 RSA Cryptosystem 6
2.3 Shamir's Three Pass Protocol 7
2.4 Conclusion 9
CHAPTER 3: METHODOLOGY AND IMPLEMENTATION **10**
3.1 Introduction 10
3.2 RSA Cryptosystem 10
3.3 Multi-Prime RSA 11
3.4 RSA Digital Signature 11
3.5 Shamir's Three Pass Protocol 12
3.6 Proposed Method 13
CHAPTER 4: RESULTS AND DISCUSSION **15**
4.1 Key Generation 15
4.2 Encryption and Decryption 15
CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS **17**
5.1 Conclusions 17
5.2 Recommendations 17
REFERENCES **18**

LIST OF FIGURES

Figure 1: Input and Output of python for encryption and decryption process..... 16

ABSTRACT

Cryptography is a study or practice of secure communication that allow only the sender and the intended recipient which can help to avoid security issues. Cryptography converts the original message, which is called plaintext, into gibberish which is known as ciphertext through certain methods. The message is then sent to the recipient in this form, then the recipient can convert the ciphertext into plaintext using the same or different key to convert it back to plaintext and get the original message. RSA Cryptography is able to verify the receiver of the message but the sender can be a third-party member. RSA Digital Signature is able to verify the sender but the receiver can be a third-party member. Shamir's Three Pass Protocol is able to make exchanging messages cannot be broken by third-party members however there is no way to verify the sender or receiver of the message. The objective of the study is to develop a modified multi-prime RSA digital signature cryptosystem and implement the multi-prime RSA digital signature cryptosystem into Shamir's Three Pass Protocol. The methodology is sending the messages using Shamir's Three Pass Protocol but the encrypted message will be signed using RSA digital signature method to be able to verify the sender and receiver. The study is hopefully able to help in boosting the security level in cybersecurity sectors.