UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

IMPLEMENTING STATION-TO-STATION PROTOCOL USING MULTI PRIME RSA CRYPTOSYSTEM

MUHAMMAD ARIF MUSA BIN ABDULLAH - 2020976723

P66M23

Report submitted in partial fulfilment of the requirement

for the degree of

Bachelor of Science (Hons.) (Mathematics)

College of Computing, Informatics and Mathematics

AUGUST 2023

ACKNOWLEDGEMENTS

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

Firstly, We are 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.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Diffie–Hellman key exchange method allows two people that have no previous knowledge of each other to jointly create a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher. However, the Diffie-Hellman protocol has a weakness in that it can easily be bypassed by a man-in-the-middle attack. Station-to-Station protocol is a protocol based on the Diffie-Hellman key exchange to prevent the man-in-the-middle attack by inserting authentication. The objectives of the study are to implement Multi Prime RSA Cryptosystem into Station-to-Station protocol and to build a system in python for the proposed method. In this study, the Station-to-Station protocol will use three (3) prime numbers Multi-Prime RSA Digital Signature. The messages will be in form of numbers, which will allow us to have verification of the sender and receiver. The mathematics concept that will be used is prime factorization and discrete logarithm problem. There is no hashing function will involve in the digital signature. The calculation during the encryption and decryption process will be handled using Python programming. The results involve the verification of the proposed method and mathematical example using three (3) prime numbers. The result will also produce the algorithm for implementing Multi Prime RSA cryptosystem into Station-to-Station protocol. It will include the coding of python programming coding and calculation of proposed method. The study recommends to use another type of digital signature algorithm to be used in the proposed method. Another recommendation is to modify and optimise the python coding in the study to be more robust and suitable for real world application.