

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

TABLE OF CONTENTS	iii
LIST OF FIGURES	iv
ABSTRACT	v
CHAPTER 1: INTRODUCTON	6
1.1 Motivation	6
1.2 Problem Statement.....	8
1.3 Objectives	9
1.4 Significant and Benefits of the study.....	9
1.5 Scope and Limitation of Study	9
CHAPTER 2: BACKGROUND THEORY AND LITERATURE REVIEW	10
2.1 RSA Cryptosystem.....	10
2.2 Diffie Hellman Key Exchange.....	11
CHAPTER 3: METHODOLOGY AND IMPLEMENTATION	12
3.1 Overview.....	12
3.2 Literature studies.....	12
3.3 Implementing Multi Prime RSA into Station-to-Station protocol	17
3.4 Build a system in python to use Multi Prime RSA cryptosystem in Station-to-Station protocol	19
CHAPTER 4: RESULTS AND DISCUSSION	24
4.1 Implementing Multi Prime RSA into Station-to-Station Protocol	24
4.2 Verification of proposed method	27
4.3 Mathematical example	29
4.4 Python Calculation.....	30
4.5 Python system Built for Implementing Multi Prime RSA into Station-to-Station Protocol	32
CHAPTER 5: CONCLUSIONS AND RECOMMENDATION	34
REFERENCES	35
APPENDIX A	37

LIST OF FIGURES

Figure 1: Process of the study	12
Figure 2: RSA Cryptosystem.	14
Figure 3: RSA Digital Signature.	15
Figure 4: Station-to-Station protocol.	16
Figure 5: Station-to-Station protocol using Multi Prime RSA Cryptosystem.	18
Figure 6: Import python modules	19
Figure 7: Create function to generate prime number	20
Figure 8: Create function to calculate Greatest Common Divisor (GCD).....	20
Figure 9: Create function for finding modular inverse	20
Figure 10: Create function for Diffie-Hellman Key Generation	21
Figure 11: Function for generating random distinct RSA prime numbers	21
Figure 12: calculate product of prime numbers	22
Figure 13: Function to generate public key	22
Figure 14: Function to calculate private keys	22
Figure 15: Showing the results of all generated values	23
Figure 16: methodology of proposed method.	25
Figure 17: Verification of the proposed method using equations.....	28
Figure 18: Coding in Python to handle calculation.	31
Figure 19: Results obtained using Python.	32

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.