UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

IMPLEMENTATION ON RSA SCHEME AND SHAMIR'S THREE PASS SCHEME WITH HILL CIPHER FOR DATA ENCRYPTION AND DECRYPTION

NURR AIDA BINTI NOR HISAM - 2020898486
NUR FARAH NABILLA BINTI NIZAR - 2020878448
NUR FATIHA AZIZAH BINTI NOORAZLAN - 2020495714

P60M23

Report submitted in partial fulfillment 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 study successfully.

We want to take this opportunity to express my deepest appreciation for everyone those who helped with the successful completion of this project, with a special word of thanks going to our lecturer, Dr Zahari bin MD Rodzi and not to forget our supervisor, Madam Nur Lina binti Abdullah.

Finally, we would like to express our gratitude to our family for their spiritual and material support throughout the writing of this study. Due to these obligations, we were able to finish this case study on schedule.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

In today's digital environment, data transmission and storage security and privacy are essential. The RSA scheme, Shamir's Three-Pass Scheme, and the Hill Cipher are three effective cryptographic approaches that are implemented in this study. Using a public-private key pair and the RSA scheme, which is based on prime numbers, secure key exchange and data encryption become possible. Shamir's Three-Pass Scheme establishes a shared secret key without the chance of interception through three rounds of communication between sender and recipient. Multiple letters are encrypted simultaneously using the polygraphic substitution cipher known as The Hill Cipher. The proposed approach demonstrates the way of various cryptographic schemes can be used effectively to enable secure communication and the protection of sensitive data. Data encryption using RSA and Hill Cypher, safe key exchange using Shamir's Three-Pass Scheme, and subsequent decryption using the proper schemes provide practical implementation. The purpose of this study is to give some exposure regarding research on the implementation of RSA and Shamir's Three-Pass Scheme with Hill Cipher for Data Encryption and Decryption. In this study, the combined RSA with Shamir's Three-Pass Scheme using a 3x3 matrix is used to generate the encryption on RSA to increase the level of security in data encryption. From the result, the combination with Hill Cipher obtained the final decrypted plaintext, which is the same message sent by the sender. From the implementation that can be done, this study also makes other calculations using different matrix conditions to see if different matrix conditions can be used for the calculation of the combination of these three schemes.