UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

IMPROVEMENT OF KEY EXCHANGE CRYPTOSYSTEM USING MATRIX WITH THREE-PASS PROTOCOL

PS39S18

ANNUUR ZAKIAH BINTI ZAINOL
FARAH DEENA BINTI MOHAMAD FISAL
FATIN NUR ATHIRAH BINTI MOHD RADZI

Bachelor of Science (Hons.) Computational Mathematics
Faculty of Computer and Mathematical Sciences

DECEMBER 2018

ACKNOWLEDGEMENTS

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

Firstly, we are grateful to Allah S.W.T for giving us the strength to complete this project successfully.

We would like to express our gratitude to our supervisors, Miss Nur Lina Abdullah for giving us guidance support and encouragement during our study. This study cannot be done without the effort and cooperation from the group members Annuur Zakiah, Farah Deena and Fatin Nur Athirah. Last but not least, we would like to thank to our friends and families who are in one way support either mentally, orally and financially.

TABLE OF CONTENTS

ABSTRACT

These days, people need a more secure ways to share important message secretly. Public-key exchange cryptographic and encryption technique in Hill Cipher are one of the secured ways that people can use to share their message. No matter how hard to break the system, advisory always find a way to dismantle the message. Therefore, cryptosystem needs improvement from time to time. In the previous work of the research paper by Kester (2012), there are only one encryption process in public-key exchange. In this study, we concerning to increase the number of encryption in order to be difficult to break. In three-pass protocol, parties uses private encryption key to generate a cipher text. However, advisory can easily attack and obtain the private encryption key. Whereas, the private encryption and decryption key will act as a public key. Throughout this research paper, mathematical method that we use to generate public key and private key are matrix.