UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

A MODIFICATION OF SHAMIR'S THREE-PASS PROTOCOL BY IMPLEMENTING ONE-TIME PAD ALGORITHM

P16S19

NUR KHAIRUNNISA' BINTI KUSMAN (2017738581)
NURUL HANIS BINTI ABD RASHID (2017390457)
AN NUR AMEERA BINTI ZAMANI (2017997401)

Report submitted in partial fulfilment of the requirement
for the degree of
Bachelor of Science (Hons.) Computational Mathematics
Faculty of Computer and Mathematical Sciences

DECEMBER 2019

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 successfully complete this report.

Sincerely thankful, we would like to express our gratitude to all of those respected people who have been giving any kind of assistance and guidance who deserve our biggest appreciation while doing our final year report. Completing this report become easier and provide us a great deal of enjoyment.

We would like to thank our supervisor, Sir Md Nizam Udin and Miss Zati Aqmar Binti Zaharudin, MSP660 lecturer for patiently providing us a guideline for this case study throughout many consultations.

Many individuals, especially our classmates, families and team members itself, for useful comments and feedback on this case study encouraged us to develop our case study. We would also like to expand our greatest gratitude to all those who have directly and indirectly guided us to finish this case study.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Shamir`s three-pass protocol is one of the methods that grants one party to send a message to another party without exchange any keys in the encryption and decryption process. However, the security in Shamir`s three-pass protocol provided is insufficient due to the advanced technology. In order to improve security, a proper algorithm should be implemented in the three-pass protocol by adding phases at starting and ending of the process. Hence, the unbreakable one-time pad is proposed to implement in Shamir`s three-pass protocol. The objectives of this study are to modified Shamir`s three-pass protocol by implementing one-time pad protocol and to develop Graphical User Interface (GUI) by using Maple software. As a result, this study success to develop the algorithm by implemented one-time pad in Shamir's three-pass protocol. This can be proved when the result in the algebraic calculation is the same as the result in Maple which is the message get by the receiver is exactly same as the sender.