UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

IMPLEMENTATION OF SCHNORR DIGITAL SIGNATURE INTO STATION-TO-STATION PROTOCOL

P16818

NURUL MAHIRA BINTI BUDIN
NOR HAFIKAH BINTI OTHMAN
NUR IZZATIE FARHANA BINTI AHMAD FAUZAN

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

DECEMBER 2018

ACKNOWLEDMENTS

Praised be to Allah S.W.T. the Almighty, the most Gracious, the most Merciful who has given us the powerless living soul, strength and healthiness, His guidance, to complete this final year project entitled "Implementation of Schnorr Digital Signature into Station-to-Station protocol" as the requirement to finish our study in Degree of Mathematical Science.

Through this acknowledgement, we would like to take this opportunity to convey a deep of sincere gratitude and thankful for our final year project's supervisor, Mr Md Nizam Bin Udin for all of his support, knowledge, exemplary guidance, monitoring and constant encouragement. He was always there whenever we needed his help in solving the problems related to this research.

Then, we expand our sincere thankful to our respected MSP600 lecturer, Dr. Mat Salim Bin Selamat for guiding us and shows on how a report should be written. Without his guidance and support, we can't finish our task correctly.

Besides, we want to thanks our final year projects' members. Thank you for the really great teamwork and for each of the idea that all of us has been contributed for this study which makes this finding finally succeed at the end.

It would be really unfair if we don't express our gratefulness to the lecturer, friends, families, and all for those who have directly and indirectly involved in finishing this research. The moral support that had been given for us is really unmeasurable.

TABLE OF CONTENTS

ABSTRACT

From our previous research, we found that Diffie-Hellman key exchange conceded two parties to share and build the common private key over an insecure channel. But it does not help in authenticate the communicating entities as it itself is a non-authenticated key agreement protocol and this will lead to "man-in-the-middle" attack. Then, we upgrade Diffie-Hellman into Station-to-Station (STS) protocol. However, STS doesn't have complete element as it's only a procedure method. Thus, we implement Schnorr Digital Signature into STS protocol to use Schnorr elements in completing the key exchange process. This implementation can help in avoiding intruder-in-the-middle attack and provide authentication for both parties. To put it briefly, Schnorr Digital Signature can be implemented into Station-to-Station protocol by using numerical equations and have been proved in this project by using graphical user interface (GUI). As a recommendation, in order to improve this project, the researchers may provide data integrity by using Hashing algorithm.