UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

IMPLEMENTATION OF STATION-TO-STATION PROTOCOL USING ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

P14S18

MUHAMMAD FARIS FAKHRI BIN ROZI
ALYA SYUHADA BINTI ISMAIL
EMYLIA BINTI SUHAIMI

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

DECEMBER 2018

ACKNOWLEDGEMENTS

IN THE NAME OF ALLAH, THE MOST GRACIOUS, THE MOST MERCIFUL. Firstly, Alhamdulillah. We are grateful to Allah S.W.T for His Faithfulness and giving us the opportunity to finish this Final Year Project successfully.

The deepest appreciation to our supervisor, Md Nizam Bin Udin who guides us for two semesters to completes this project by giving the continued support, the consultation also the guidelines for this project. Without his encouragement, it is hard for us to finish this project perfectly.

Special thanks also to those people who directly or indirectly helped in the project. Their help that consists of sharing idea and information helps us a lot to build up the perfection in this project.

Last but not least, thanks for our parent that always support us in a various way. They are the people that give us an inspiration and build our spirit to complete this project.

TABLE OF CONTENTS

ABSTRACT

Diffie-Hellman key exchange is a protocol to exchange key between two parties. Unfortunately, the Diffie-Hellman protocol is not save from intruder such as Man-In-The –Middle (MITM) attack because it allows two parties changing the secret key to an unsecured communication without any meeting due to Diffie-Hellman key exchange does not have an authentication element. Elliptic Curve Digital Signature Algorithms (ECDSA) is implemented in Station-To-Station protocol in order to give an improvement in the secret key exchange between two parties. This protocol will provide an element of authentication element and data integrity in the system. This project was developed into a Graphical User Interface (GUI) using MAPLE software to show how the system works. It was believed that this implementation has increased the level of secrecy in the sharing session using the method applied. Throughout this study another improvement is recommended to be applied in order to provide data integrity into the system as current scope of the study only focus on the element of authentication.