UNIVERSITI TEKNOLOGI MARA

ENCRYPTED MOBILE MESSAGING APPLICATION USING 3D-AES BLOCK CIPHER CRYPTOGRAPHY ALGORITHM

AIDA NAJIHAH BINTI MOHD KHLUBI

BACHELOR OF COMPUTER SCIENCE (HONS.)

JULY 2019

ACKNOWLEDGEMENT

Alhamdulillah, praises and thanks to Allah SWT because of His Almighty and His utmost blessings, I was able to finish this research proposal within the time duration give. Firstly, my special thanks goes to my supervisor, Associate Professor Ts Dr Suriyani Ariffin for guiding me to complete this research proposal successfully.

Secondly, I would like to offer my gratitude to my CSP650 lecturer, Dr Marina Ismail. My appreciation also goes to all my lecturers that have taught me throughout my degree years in UiTM Shah Alam. Special appreciation also goes to my beloved parents for all the moral support given in order for me to accomplish this proposal successfully.

Last but not least, I would like to give my gratitude to my dearest friends that have helped me by giving their ideas for me to complete this proposal.

ABSTRACT

This paper analyzes how information sent through mobile messaging application is being secured. Nowadays, people are more likely to communicate with each other through mobile application. There is a high possibility that the information could have been leaked to intruders. It is crucial to maintain the confidentiality and privacy of the information. Therefore, securing the information sent via mobile messaging application is important by implying the cryptography technique. Cryptography technique comprises encrypting and decrypting information which can only be seen by the sender and receiver. This paper focusing on encrypting and decrypting text sent through the application. The process of securing the text is by using the 3Dimensional-Advanced Encryption Standard (3D-AES) block cipher algorithm. Android Studio software is used in developing the project. The data involved is stored in database by using Firebase database. The text will be encrypted first before sending it to the intended receiver. A specific key is used to encrypt and decrypt the text, which can only be known and accessed between the sender and receiver. The result of this project is based on the efficiency of securing the messages through encrypting and decrypting them. This project provides protection to any personal conversations between the sender and the receiver and it secure the people's personal information by applying the encryption and decryption method.

TABLE OF CONTENTS

CONTENT **PAGE**

CHAPTER 2

LITERATURE REVIEW

In this chapter, the literatures from the various researches will be discussed. Various beneficial articles that contain information related to this project will be reviewed in this chapter. This literature assists and provides useful and valuable information in the process of developing this project.

2.1 Cryptography

Cryptography is the art of writing or solving codes that allows any information to be sent is in a protected form, where only the intended person able to retrieve the information (Benni & Hetty, 2015). According to Pandey and Verma (2015), a process of encryption and decryption messages or data which only the authorized users can understand is called cryptography. It offers several functions such as provides privacy or confidentiality, authentication, integrity, non-repudiation, and key exchange.

According to Kessler (2018), five primary functions of cryptography are privacy or confidentiality, authentication, integrity, non-repudiation, and key exchange. Firstly, privacy and confidentiality is to ensure that only the intended receiver can read the message. Next, authentication is a process of verifying one's identity. Then, integrity is to ensure that when receiver has received the message, it will not be altered from its original form. Non-repudiation is a mechanism to confirm that the sender really sent the message. Lastly, key exchange is a procedure in which the crypto keys are shared between the sender and receiver. There are three