Universiti Teknologi MARA

Enhancement of Text-Based Advanced Encryption Standard Algorithm (AES) in the Android Platform

Mohamad Zakirin Bin Mohammad Zahari

Thesis submitted in fulfilment of the requirements for
Bachelor of Science (Hons) Computer Science
Faculty of Computer and Mathematical Sciences

January 2014

ACKNOWLEDGEMENT

Assalamualaikum and Alhamdulillah, thanks to Allah SWT, whom giving me the time and opportunity to complete this Final Year Project with the title Enhancement Of Text-Based Advanced Encryption Standard Algorithm (AES) In The Android Platform. I have taken efforts in this project but it would not been done without the support and help of many individuals. I would like to extend my sincere thanks to all of them.

Firstly, I would like to give my special thanks of gratitude to my lecturer, Madam Siti Khatijah Nor Binti Abdul Rahim and Mr Mohamed Imran Bin Mohamed Arif and also to my supervisor, Miss Samsiah Binti Ahmad who had monitoring and advise me from the beginning and also give a guidance and support to finish this project. Their advice and support all trough in completing this Final Year Project report was very guide me to settle this project on time. They never give up in supporting me and also spend a lot of time with me even they are busy with their own works and life. I am very grateful to have my lecturers and my supervisor.

Besides, a lot of thanks and appreciate also to my parents, family, housemate, and friends for their encouragement, cooperation, advises and support for this project completion, from the beginning until now. Everyone has been contributed by supporting my work, give ideas and also help me during the progress of my project until it is completed. All the comments and advices from all of them were really effective to keep me stayed focus and keep improvised my works from time to time. Thanks.

ABSTRACT

Cryptography is a one of the method to provide the secrecy of information or data. Nowadays, there are a lot of cryptography method has been applied. One of the most popular cryptography methods is Advance Encryption Standard (AES). On this paper, the research will focus on the AES encryption and decryption computational process of the text in the Android platform. AES algorithm been chosen because it is one of the most secured cryptography methods, very flexible, and most commonly implemented. However, AES users or application that using AES algorithm might face the problem of computational overhead. The enhanced AES-128 bit algorithm was omitted the mix column step from second round until the ninth round and being replaced with shift row step. This will help to speed up the algorithm because mix column step was using high calculation and needs a lot of time to process it. Based on the research that had been conducted, it shows that the enhanced algorithm have managed to speed up the computational process for encryption and decryption of the text in the Android platform to reduce computational overhead. Therefore, hopefully in future, any cryptography developers can implement this code if they want to encrypt the complex data. In future, the test toward the strength of this enhanced AES-128 bit algorithm should be conducted.

TABLE OF CONTENT