Universiti Teknologi MARA

Audio Encryption and Decryption Using 3D AES Block Cipher Algorithm

Nur Fattin Nadhrah Binti Saifuddin

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

January 2018

ACKNOWLEDGEMENT

Alhamdulillah, praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given. Firstly, my special thanks goes to my supervisor, Dr. Suriyani Ariffin who acts as advisor in accomplish my project. A very big thanks to her for giving instruction, advices, support and guides in obtaining a good research.

Special appreciation also goes to my beloved parents, Saifuddin Bin Sulaiman and who always very understanding and support in any kind situation. They keep give their presence, encouragement, and understanding, in order to finish this project.

Last but not least, I would like to give gratitude to my dearest friends for being helping, support and encouragement to complete this project.

ABSTRACT

Nowadays, people are usually send the data via Internet or thumb drive instead of using letter. Especially for audio data, people are not sending audio using letter but send it over the radio channel or internet devices in order to receiver can hear it well. Besides, how to keep the audio as a secret if people can send it and receive it very well? Audio encryption and decryption introduce the process where we can keep the data secret, only for sender and receiver can accept the message. The audio will be encrypt to unknown message and will be decrypt by receiver using secret key. This technique will be tested in order to compare with other research. This project purpose is to identify the implementation testing security using 3D AES block cipher algorithm. Besides, this encryption using audio as a data in order to design and develop the project. This project also measure the security analysis on linearity test. In other and, ADDIE model is a methodology that including analysis, design, development, implementation and evaluation that complete the cycle of the project that starts from get the title of project, survey and collect the information about encryption and decryption, and specify the scope to 3D AES block cipher algorithm.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Chapter one explains about background of study where the information can come in any kind of versions which is text, video, image or audio. What if no encryption and decryption while transferring data? The data might be leak to others or high risk to get the information. Besides, this chapter have to identify the implementation of testing security analysis. Besides, the design and development the encryption and decryption in audio using 3D AES block cipher algorithm and measure the security analysis on linearity test. This system can be used by government, military or any confidential company that needs to transfer the information.

1.1 Background of study

Nowadays, the information or the data can be in many kind of versions. Not only in a text, but also can be in a video, an image or an audio. The information is being shared worldwide since the internet are slowly grown up and became as the source to share the data. So, the encryption and decryption method needed to keep the specific information hidden from the unknown sources.

The concept of encryption and decryption is to process the information into the hidden one and decryption is convert the encrypt information or hidden data to the original so that the user can read the contain of the data.

In this project, the encryption and decryption of the data are using 3D AES. According to Singh and Supriya (2014), AES is the encryption standard that can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. AES and 3D AES is different because 3D AES composed of rotation key function, minimum 3 iterations of round function and key mixing operations (Ariffin,2013).