UNIVERSITI TEKNOLOGI MARA

DATA PRIVACY COMPARISON USING ADVANCED ENCRYPTION STANDARD (AES) AND DATA ENCRYPTION STANDARD (DES)

HIKMA FARAH ALI

MSc

January 2019

ABSTRACT

Cryptography has wide ranges as it has the ability to handle different attacks. It has a set of security objectives to ensure the confidentiality of data. This changes the content of the data being sent to a readable form once received by the recipient and is converted back to its original form. Using this project for generated key for protect the file. The file is encrypted and using this key to decrypt it. In this study existing algorithm DES is a symmetric-key block cipher. DES creates 64 bit cipher text and produces 64-bit block of plaintext. As encryption and decryption of DES uses same cipher key by 56 bit. Proposed algorithm AES, has a different key sizes ,as 128,192 and 256. DES has weak keys. For avoiding the issues in DES, we propose, AES which is a stronger key schedule should prevent weak keys. In this project using the AES algorithm, it benefits to encryption and decryption and it avoids the time delay. Our aim is to safely to transfer the file for using the AES algorithm. Proposed algorithm has done by analysing the different time taken for both AES and DES , experiment was done by three different file sizes and also file types, such as text, image and voice to test the encryption and decryption time taken on existing algorithm DES and proposed algorithm, in conclusion, all the results of our propose algorithm shows AES takes lesser time compare to DES. Our propose also compare the key bit size of existing algorithm DES and Proposed algorithm AES. Finally our result show the AES has strong key compare to DES.

ACKNOWLEDGEMENT

ALHAMDULILLAH, my appreciation first goes to Allah SWT whom in His infinite mercy has given me the opportunity to complete this dissertation which is title “Data Privacy Comparison using Advanced Encryption Standard (AES) and Data Encryption Standard (DES)”. I would like to thank all the wonderful people who supported and encouragement me this dissertation. My gratitude goes to my wonderful, all time hearing and caring dissertation supervisor, Dr. Zolidah kasiran for her ultimate support, expertise and patience during all stages of my dissertation. Her advices were very useful and encouraging in motivating me to complete my project. I am also indebted to Universiti Teknologi MARA (UITM) and other lecturers who gave me their advice.

Secondly, my humble appreciation to family my beloved parent Haji Farah Ali and the sweetest mother on earth Fadumo Abdi Adan, my wonderful husband, Ahmed Abdullahi Osman and my dear sisters and brother Qadro, Qamar, Hussain Farah Ali who always support me financially and spiritually and lives me with no choice than to dedicate this dissertation to them for fulfilling their dream for which they have been waiting for this moment for a long time.

Special thanks to my colleagues and friends for helping me with this project.

TABLE OF CONTENT

CHAPTER ONE
INTRODUCTION

1.1 Research Background

With the advancement of technology, attacks are also increasing at an important rate. Today, most of the information is transmitted via a communication channel like the Internet because both senders and recipients are simple and convenient channels. Therefore, the need for security is always a major problem. If an intruder presses data, it can cause uncreatable damage. For this reason, many ways have been proposed to protect the information that is broadcast and received on unsafe channels. Now every potential machine can be hacked to get confidential data. To protect data from various attacks, many encryption methods are evolving and before transmission, we must logically encrypt the data to ensure integrity. Due to the widespread usage and sharing of data on the Internet, data needs to be protected from hacker's interference. However, an attacker can capture important data because the communication channel is not secure. Security is essential for any area requiring data exchange, especially the most important data such as transactions. This problem is related to institutions like universities, business organizations, and government agencies.

In the current technology, data leakage is considered a huge test for various basic industries. To work around this problem, a set of information security templates was created using many cryptographic algorithms (P. R. M. Rao, 2017). Availability of the Internet and emerging technologies such as social networks and smartphones to ensure the privacy of data in the case despite the exchange of data between partners who are not reliable for the purposes of analysis, general data must be restructured to avoid data users from reallocating shared data to others without the consent of the data provider. Protecting sensitive information for individuals is critical. Also, data is increasingly important.

If information is leaked, it may affect individuals based on information sensitivity. In order to maintain the privacy of data sharing data, the shared data cannot be stored directly in the data lake (Scoon, 2016). Otherwise, the Administrator may cause the data to leak to unauthorized data users without the consent of the corresponding data provider.