UNIVERSITI TEKNOLOGI MARA

FINAL EXAM QUESTION PAPER DATA ENCRYPTION AND DECRYPTION USING ADVANCE ENCRYPTION STANDARD

KHAIRUL NASHRAN BIN NAZARI

BACHELOR OF COMPUTER SCIENCE (HONS.)

JANUARY 2017

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, Mr Mazlan Bin Osman who has helped, supported and guided me throughout my research. Special appreciation also goes to my beloved parents who have given me wonderful ideas, unparalleled motivation and support throughout my studies. Last but not least, I would like to extend my gratitude to my dearest lecturers and friends who have helped me during my degree study.

ABSTRACT

Nowadays, electric documents are considered as an easier way to communicate between two parties. However, the documents may contain sensitive information that is valuable to attackers. Most of the organizations nowadays stored their secret documents in their online database. This means that it is accessible for the authorized user in their organization and vulnerable to cyber-attacks which are threatening the secrecy of the documents and organizations. In this research, the final exam question papers prepared by Universiti Teknologi MARA (UiTM) are proposed to be encrypted using Advanced Encryption Standard (AES) for online distribution. Final exam question papers are also secret documents which fall under information security as UiTM is currently distributing the question papers manually from UiTM Shah Alam to its branches. With the implementation of AES, the question papers will be able to be distributed using online services such as emails or cloud storage. The distribution using online services will cut the cost of distributing and communications in the organizations. AES is a data encryption technique that exist in the world with as currently the most secured algorithms. AES is the next generation encryption algorithm replacing the older version which is DES and Triple DES. AES is being used widely in many applications since it is known for its faster encryption and decryption process and its strength. AES in this research was implemented using 128-bit of key length and block size. The overall transformation encryption process consist of iterative steps called rounds. A 128-bit key requires 10 rounds where 192-bit and 256-bit requires 12 and 14 rounds respectively. The steps involved are SubBytes, ShiftRows, MixColumns and AddRoundKeys. This technique is then compared to DES, 3DES and Blowfish to verify and measure the effectiveness of the AES. The results from this research have proved that the AES is very effective in terms of time taken to encrypt and decrypt documents, strength of the algorithm and the reliability of the program. It is recommended that Final Examination Question Papers be enhanced using Encryptor Application by applying AES on a different domain to further strengthen information security.

TABLE OF CONTENTS