ABSTRACT

The problem of security and confidentiality is one of the most important aspects of the data. One way to keep that is using encoding technique called cryptography. Cryptography is usually implemented on text data. That is why this Final Project will do a research about cryptography in text file.

Cryptography system used in this Final Project is hybrid cryptosystem, which combined symmetric cryptography with asymmetric cryptography. For symmetric cryptography, it uses DES algorithm (by using four block cipher modes of operation that is ECB, CBC, CFB, and OFB). Meanwhile, for asymmetric cryptography is using RSA algorithm. The reason why hybrid cryptosystem is chosen is fast processing of the data using symmetric algorithm and to simplify key management using asymmetric algorithm.

From data the testing results obtained by the encryption average time per character of DES key by using RSA 512 bit and 1024 bit, that is equal 1.937 ms and 5.537 ms. Meanwhile, the encryption average time per character of text data by using ECB mode that is equal 0.041525 ms, whereas by using the CBC/CFB/OFB mode that is equal 0.044419 ms. From these measurements that the increasing length of RSA key makes the generation time for RSA key and processing time of encryption/decryption DES key increasing too, and memory usage increasing too. Processing time and memory usage measurement in operation mode, we get the score: ECB<CBC≈CFB≈OFB. Meanwhile, the result of system robustness testing using avalanche effect method concluded that the best result is found in CBC operation mode. Based on system testing using black box test and beta test, the conclusion is that the system already run in accordance with the algorithm principle used in this research, that are DES and RSA with sample process to secure text data file.

Key word: hybrid cryptosystem, cryptography, encryption, decryption, block cipher modes of operation, RSA, ECB, CBC, CFB, OFB, symetric, asymmetric.