ABSTRACT

The information and data security is very important in data transfer process, one way of securing data is by using cryptographic methods. Cryptography is the science that studies mathematical techniques related to aspects of information security, such as data confidentiality, data authenticity, data integrity, and data authentication. Transmitted data can be public or confidential information.

In this final project, a design of cryptographic key modified algorithms RC6 in the form of Java applications is created. The input of the application is a text, then the text is encrypted and decrypted using the algorithm RC6 with a regular key. And then, the encryption and decryption process is carried out using the RC6 algorithm with a key that has been modified. The modified key is enabled with Blum-Blum Shub.

The used of RC6 algorithm has a good performance, seen from the regular key RC6 Avalanche Effect in the range of from 46 875% to 65 625% and the value of the modification key RC6 Avalanche Effect in the range of 43.75% to 62.5%. Average time for the ordinary RC6 encryption key is 3.94939 seconds and the average time for the modification RC6 encryption key is 3.72655 seconds. The average memory used for regular key RC6 is 20 MB and the average memory used for modified RC6 key is 23 MB. It can be concluded that the encryption time of modified RC6 encryption key is faster than the ordinary RC6 encryption key and memory used for modified key RC6 is bigger than the memory used in regular RC6 key.

Keywords: Text File, Cryptography, RC6 Algorithm, Blum – Blum Shub