ABSTRACT

One of the methods to securing data or information inside a document file is cryptography. Cryptography is the study of technique to securing data communication, without unauthorized access from third party. The data sent might be general or secret information.

This final project is focused on designing a modification on Twofish cryptography algorithm. The plaintext is encrypted and decrypted with normal Twofish algorithm. Then the inputted plaintext will be encrypted and decrypted using key modified of Twofish algorithm. The modification done is on the key. The key inputted by user will act as the input for a formula, with output from Blum Blum Shub.

From the testing results, the algorithm is having good performance. The Avalanche Effect is between 0,41 – 0,63. The average encryption time for standard Twofish is 19,375107 second, while The average encryption time for key modified Twofish is 13,835254 second. From the result it can be known that the time used for encryption with key modified Twofish algorithm is faster than standard Twofish algorithm. The average memory used for standard Twofish is 17.06667 MB, while the average memory used for key modified Twofish is 25.63333 MB. From the result it can be known that while measuring the computation memory, the key modified Twofish algorithm is using more memory.

Keywords: Text file, Cryptography, Twofish algorithm, Blum Blum Shub