ABSTRACT

DES algorithm developed at IBM (International Business Machines) under the leadership of WL Tuchman in 1972. The algorithm is based on the Lucifer algorithm created by Horst Fiestel. The first DES algorithm has 56-bit key length. With this 56-bit key length, DES weak against exhaustive key search attack or by trying all possible keys.

At the end of the project has developed the DES algorithm with the expansion along the 112-bit key. Development is carried out by adding a network fiestel into 4 blocks that were previously only 2 blocks.

Results of analysis showed that the modified DES with 112-bit key length of time exhaustive key search has 256 times the original DES with 56-bit key length. The results of the demonstration showed that the modified DES encryption Shannon meets the two principles of confussion and diffusion.

Keywords: Block cipher, DES, decryption, encryption