

Abstract

Cryptography, since it's founded, has grows in many different algorithm with each excess and shortage. In 1998, cryptography algorithm Rijndael has chosen as Advanced Encryption Standard (AES) in the contest which held by National Institute of Standards and Technology (NIST). This algorithm is designed by Vincent Rijmen and Joan Daemen. One of AES designer, Vincent Rijmen, with Paulo S. L. M. Baretto, built a new cryptography algorithm named Anubis in 2000, which have similar structural with Rijndael cryptography algorithm.

From the both of algorithm not known yet which algorithm is the best. That's why in this Final Project will be done an examination for comparing both of cryptography algorithm. This examination will be implemented in software with three parameters. They are time of process, memory usage, and avalanche effect. From the result of examination with time of process and memory usage parameters, Anubis cryptography algorithm is better than Rijndael. For avalanche effect parameter, in same plaintext with different key condition, Rijndael cryptography algorithm is better than Anubis. But in same key with different plaintext condition, Anubis cryptography algorithm is better than Rijndael.

Key words: cryptography, block cipher, anubis, rijndael, memory, avalanche effect.