

Abstrak

Sejak ditemukan, kriptografi sebagai telah berkembang menjadi beragam algoritma yang masing-masing memiliki kelebihan dan kekurangan. Pada tahun 1998, algoritma kriptografi Rijndael terpilih sebagai *Advanced Encryption Standard* (AES) dalam kontes yang diadakan oleh *National Institute of Standards and Technology* (NIST). Desainer dari algoritma ini adalah Vincent Rijmen dan Joan Daemen. Pada tahun 2000, salah seorang dari desainer AES, Vincent Rijmen, bersama Paulo S. L. M. Baretto, membuat sebuah algoritma kriptografi baru yang diberi nama Anubis, yang memiliki kemiripan struktural dengan algoritma kriptografi Rijndael.

Dari kedua algoritma kriptografi tersebut belum diketahui yang mana yang lebih baik. Sehingga pada Tugas Akhir ini akan dilakukan pengujian untuk membandingkan kedua algoritma kriptografi tersebut. Pengujian ini diimplementasikan dalam bentuk perangkat lunak dengan tiga parameter. Parameter-parameter tersebut adalah waktu proses, memori yang digunakan, dan *avalanche effect*. Dari hasil pengujian untuk parameter waktu proses dan pemakaian ruang memori, algoritma kriptografi Anubis lebih unggul. Untuk parameter *avalanche effect*, pada kondisi plainteks yang sama dengan kunci berbeda, algoritma Rijndael lebih baik daripada Anubis. Sedangkan untuk kondisi kunci yang sama dengan plainteks yang berbeda, algoritma kriptografi Anubis lebih baik daripada Rijndael.

Kata kunci: kriptografi, *cipher* blok, anubis, rijndael, memori, *avalanche effect*.