ABSTRAK

Untuk menjaga keamanan suatu data atau informasi yang tersimpan dalam bentuk file dokumen terdapat metode tertentu, salah satunya adalah kriptografi. Kriptografi adalah ilmu yang mempelajari cara untuk menjaga keamanan data agar tetap aman saat dikirimkan, tanpa mengalami gangguan dari pihak ketiga. Data yang dikirimkan bisa berupa informasi umum atau rahasia.

Dalam tugas akhir ini dilakukan suatu perancangan untuk memodifikasi kunci algoritma kriptografi Twofish. Teks dienkripsi dan didekripsi dengan menggunakan algoritma Twofish standar. Setelah proses enkripsi berhasil teks masukan akan dienkripsi dan didekripsi dengan menggunakan algoritma Twofish yang telah dimodif kuncinya. Bagian yang dimodif dari algoritma Twofish adalah pada bagian kuncinya yang difungsikan dengan Blum Blum Shub.

Algoritma Twofish yang digunakan memiliki performansi yang baik, terlihat dari nilai *Avalanche Effect* yang diberikan berkisar antara 0,41 – 0,63. Waktu rata-rata yang digunakan untuk proses enkripsi algoritma Twofish standar adalah 19,375107 detik, sedangkan waktu rata-rata yang diperlukan untuk proses enkripsi pada algoritma Twofish modifikasi kunci adalah 13,835254 detik. Jadi dapat dilihat dari hasil tersebut bahwa waktu yang digunakan pada proses enkripsi dengan menggunakan Algoritma Twofish modifikasi kunci lebih cepat jika dibandingkan dengan algoritma Twofish standar. Memori rata-rata yang digunakan pada algoritma Twofish standar adalah 17,06667 MB, sedangkan memori rata-rata yang digunakan untuk Algoritma Twofish modifikasi kunci adalah 25,63333 MB. Dapat dilihat dari hasil di samping bahwa pada saat penghitungan memori komputasi terlihat bahwa algoritma Twofish kunci modif membutuhkan memori lebih banyak.

Kata Kunci : File teks, Kriptografi, Algoritma Twofish, Blum Blum Shub