

ABSTRAK

Keamanan suatu data atau informasi berupa file dokumen sangat penting, salah satu cara pengamanan data adalah dengan menggunakan metode kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Data yang dikirimkan bisa berupa informasi umum atau rahasia.

Dalam tugas akhir ini dibuat suatu perancangan algoritma kriptografi RC6 yang dimodifikasi kuncinya dalam bentuk aplikasi Java. Masukan dari aplikasi tersebut adalah teks, kemudian teks dienkripsi dan didekripsi menggunakan algoritma RC6 dengan kunci biasa. Terakhir, dilakukan proses enkripsi dan dekripsi menggunakan algoritma RC6 dengan kunci yang telah dimodifikasi. Kunci yang dimodifikasi yakni kunci yang difungsikan dengan *Blum Blum Shub*.

Algoritma RC6 yang digunakan memiliki performansi yang baik, terlihat dari nilai *Avalanche Effect* kunci biasa RC6 yang diberikan berkisar antara 46.875% sampai 65.625% dan nilai *Avalanche Effect* kunci modifikasi RC6 yang diberikan berkisar antara 43.75% sampai 62.5%. Rata-rata waktu enkripsi kunci biasa RC6 yang dihasilkan yaitu 3.94939 detik dan rata-rata waktu enkripsi kunci modifikasi RC6 yang dihasilkan yaitu 3.72655 detik. Rata-rata memori kunci biasa RC6 yang digunakan yaitu 20 MB dan rata-rata memori kunci modifikasi RC6 yang digunakan yaitu 23 MB. Dapat disimpulkan bahwa waktu enkripsi kunci modifikasi RC6 lebih cepat daripada waktu enkripsi kunci biasa RC6 dan memori yang digunakan kunci modifikasi RC6 lebih banyak daripada memori yang digunakan kunci biasa RC6.

Kata Kunci : File teks, Kriptografi, Algoritma RC6, *Blum- Blum Shub*