Abstrak

RC4 adalah salah satu algoritma kriptografi *stream cipher* yang masih sering digunakan pada protokol keamanan. Algoritma ini terdiri dari 3 langkah utama (inisialisasi array, ksa, dan PRGA) untuk membangkitkan suatu *keystream* yang akan digunakan dalam proses enkripsi dan dekripsi. Proses enkripsi dan dekripsi pada RC4 dilakukan dengan operasi XOR antara *keystream* dengan *plaintext*. RC4 dapat dijalankan dengan panjang kunci variable dan operasi dengan orientasi byte.

Metode enkripsi RC4 memiliki kelemahan. Kelemahan yang paling dikenal adalah *Bit-Flipping Attack* atau BFA, dimana penyerang dapat mengetahui sample atau keseluruhan *plaintext* dari *ciphertext* tanpa harus mengetahui kunci enkripsi. Pada Tugas Akhir ini di ajukan modifikasi CRC untuk mengatasi masalah *Bit Flipping Attack*. Adapun modifikasi dilakukan dengan memberikan nilai CRC-32 bit pada *plaintext* sebelum dilakukan enkripsi dan setelah proses enkripsi dihitung nilai CRC kembali.

Dari hasil pengujian yang dilakukan terhadap algoritma RC4, penambahan proses perhitungan CRC pada *plaintext* sebelum dilakukan proses enkripsi berhasil meningkatkan keamanan data dari serangan *Bit Flipping Attack*. Kualitas kriptografi RC4 Modifikasi CRC yang dihasilkan pada sistem ini dipengaruhi oleh ketahanan *avalanche effect* dan waktu proses eksekusi. Kualitas *avalanche effect* untuk kondisi *plaintext* yang sama dengan kunci yang berbeda nilai *avalanche effect* RC4 modifikasi CRC sama baiknya dengan nilai *avalanche effect* yang dihasilkan dari algoritma RC4 Modifikasi CRC pada kondisi kunci yang sama dengan *plaintext* yang berbeda. Pada algoritma RC4 panjang pesan *chipertext* lebih pendek 4 byte dibandingkan RC4 modifikasi CRC, sehingga waktu proses enkripsi/dekripsi RC4 lebih cepat dibandingkan RC4 Modifikasi CRC.

Kata Kunci: RC4, enkripsi, dekripsi, *Bit Flipping Attack*, CRC.