ABSTRAK

Wireless Fidelity atau WiFi adalah teknologi yang digunakan sebagai *Wireless Local Area Network* atau WLAN. Salah satu kendala kompetensi pada WLAN adalah kerentanan terhadap aspek keamanan jaringan. WPA-PSK adalah salah satu metode sistem keamanan jaringan *wireless* yang sudah banyak digunakan dan menggunakan algoritma RC4. Kelemahan algoritma RC4 yang paling dikenal adalah *Bit Flipping Attack* atau BFA. Serangan BFA ini bertujuan untuk mengetahui sebagian atau keseluruhan *plaintext* dari *ciphertext* tanpa harus mengetahui kunci.

Pada Tugas Akhir ini diajukan CRC-32 bit sebagai teknik untuk memberikan nilai pada *plaintext* sebelum dilakukan enkripsi. Penambahan CRC-32 pada algoritma RC4 bertujuan untuk memperkuat *plaintext* pada saat proses enkripsi. Hasil enkripsi yang berupa *ciphertext* lalu akan dikirim ke penerima. Lalu dalam pengujian, pada media *wireless*, *attacker* melakukan *Bit Flipping Attack* (BFA) dengan mengubah 1 bit dari *ciphertext* dari 0 ke 1 atau sebaliknya, saat proses pengiriman. Pada proses dekripsi akan dilakukan pengecekkan kembali apakah data yang diterima rusak atau tidak dengan cara membangkitkan kembali kunci dan pengecekkan nilai CRC cocok atau tidak.

Dari hasil pengujian yang dilakukan terhadap RC4, penambahan CRC pada *plaintext* sebelum dilakukan enkripsi berhasil meningkatkan ketahanan RC4 terhadap serangan *Bit Flipping Attack*. Kualitas dari RC4 yang sudah dimodifikasi CRC dipengaruhi oleh *avalanche effect* dan waktu komputasi saat eksekusi. Dengan menggunakan *plaintext* yang sama dengan kunci yang berbeda, serta menggunakan *plaintext* yang berbeda dengan kunci yang sama, masing-masing menghasilkan nilai *avalanche effect* yang sama baiknya, yaitu berkisar antara 45% sampai dengan 60% namun ada beberapa yang menghasilkan nilai AE kurang dari 45%, dipengaruhi oleh jumlah karakter yang berbeda, nilai key dan seed yang diinputkan dan banyaknya percobaan. Akan tetapi, kelemahan pada metode yang diajukan ini adalah waktu komputasi yang dibutuhkan untuk enkripsi / dekripsi menjadi lama dibandingkan RC4 tanpa penambahan CRC-32.

Kata Kunci : RC4, *Bit Flipping Attack*, CRC, Enkripsi, Dekripsi, *Avalanche Effect*.