ABSTRAK

UMTS (Universal Mobile Telecomunication System) merupakan sistem komunikasi nirkabel generasi ketiga yang merupakan hasil pengembangan dari GSM (Global System for Mobile Communication). Dengan semakin pesatnya perkembangan teknologi seluler (nirkabel) ini, sistem keamanannya juga semakin mendapat perhatian untuk menghindari adanya pencurian informasi oleh pihak atau badan yang tidak bertanggung jawab.

Sistem keamanan pada jaringan UMTS menggunakan kriptografi algoritma f8 dan f9 untuk menjaga kerahasiaan dan integritas data antara User Equipment (UE) dan Radio Network Controller (RNC). Algoritma f8 merupakan algoritma untuk proses enkripsi-dekripsi untuk menjaga kerahasiaan data. Sedangkan algoritma f9 adalah algoritma untuk menghasilkan kode yang ditambahkan ke data yang akan dikirim untuk menjaga integritas data. Algoritma f8 dan f9 dibuat berdasarkan algoritma block cipher KASUMI yang merupakan jenis algoritma simetri dimana kunci yang dipakai untuk proses enkripsi dan dekripsi sama dengan inputan 64-bit dan ukuran kunci 128-bit menghasilkan outputan 64-bit. Tugas akhir ini secara khusus membahas simulasi kriptografi algoritma f8 dan f9 pada UMTS dengan menggunakan Matlab 2007a. Kemudian membuktikan kemampuan sistem algoritma f8 dan f9 dengan cara menganalisa waktu dan performansi proses, serta menganalisa tingkat distribusi keacakan atau perubahan bitnya dan *avalanche effect* pada algoritma f8. Dan mengukur kehandalan algoritma f8 dan f9 dari *Brute Force Attack*.

Dari hasil pengujian dapat disimpulkan perubahan bit input dan output algoritma f8 dari beberapa kali percobaan untuk teks =53,5125%, suara=51,254%, dan gambar=49,81162%. Waktu dan performansi algoritma f8 dan f9 hampir sama. Nilai *avalanche effect* algoritma f8 berdasarkan perubahan 1 bit kunci mencapai 50,23202% sedangkan berdasarkan perubahan 1 bit *plaintext* atau *ciphertext* hanya 3,125%. Sedangkan waktu untuk melakukan *brute forced attack* pada algoritma f8 dan f9 ialah 1,618 x 10^{40} tahun.

Kata Kunci : UMTS, Algoritma f8, f9, KASUMI, brute force attack dan avalanche effect