BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini, komunikasi *mobile* sudah menyebar ke seluruh dunia dengan sangat cepat, dengan perkembangan teknologi yang tidak kalah cepat pula. Teknologi komunikasi *mobile* telah mencapai generasi ketiga (3G) dimana telah dapat melakukan transfer data suara dan data lainnya secara bersamaan. Dengan semakin pesatnya perkembangan teknologi seluler (nirkabel) ini, perhatian pada tingkat-tingkat keamanannya juga semakin mendapat perhatian. UMTS (Universal Mobile Telecomunication System) adalah sebuah standar internasional untuk sistem komunikasi *mobile* 3G yang menggunakan metode kriptografi untuk menjaga kerahasiaan informasi yang ditransmisikan antara UE (User Equipment) dan RNC (Radio Network Controller)

Sistem keamanan pada jaringan UMTS menggunakan kriptografi algoritma f8 dan f9 untuk menjaga kerahasiaan dan integritas data antara UE dan 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 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*

1.2 Tujuan Tugas Akhir

Tujuan dari tugas akhir ini adalah :

1. Membuat aplikasi simulasi algoritma f8 dan f9.
2. Membuktikan kemampuan sistem algoritma f8 dari tingkat distribusi keacakan atau perubahan bitnya, waktu dan performansi proses dan *avalanche effect*

3. Membuktikan kemampuan sistem algoritma f9 dari waktu dan performansi proses
4. Mengukur kehandalan algoritma f8 dan f9 terhadap *Brute Force Attack*.

1.3 Rumusan Masalah

Dalam Tugas akhir ini akan dibahas kriptografi algoritma f8 dan f9.

Parameter-parameter yang akan dilakukan penganalisaan dan pensimulasian :

1. Bagaimana memodelkan kriptografi algoritma f8 dan f9
2. Bagaimana perubahan bit-bit setelah proses pengenkripsian dan pendeskripsian suatu inputan data pada algoritma f8.
3. Bagaimana lamanya waktu pemrosesan dan performansi pada algoritma f8 dan f9. Serta tingkat avalanche effect akibat perubahan bit plaintext maupun kunci pada algoritma f8.
4. Bagaimana tingkat kehandalan algoritma f8 dan f9 terhadap *Brute Force Attack*

1.4 Batasan Masalah

Tugas akhir ini dibatasi pada ruang lingkup algoritma f8 dan f9. Pembahasan hanya difokuskan pada penganalisaan simulasi dengan melakukan percobaan-percobaan. Berikut batasan-batasan yang dipakai :

- Pembahasan hanya akan difokuskan pada analisis dan simulasi menggunakan kriptografi algoritma f8 dan f9
- Proses enkripsi atau dekripsi *plaintext* atau *ciphertext* menjadi *ciphertext* atau *plaintext* pada algoritma f8.
- Proses menghasilkan kode Message Authentication Code-Integrity(MAC)/XMAC-I pada algoritma f9.
- Analisis hasil enkripsi atau dekripsi algoritma f8 dengan parameter : perubahan bit, lama proses, performansi, dan *avalanche effect.*
- Analisis hasil MAC-I/XMAC-I algoritma f9 dengan parameter: lama proses dan performansi
- Tidak memperhatikan skema modulasi hingga demodulasi, kanal, dan faktor-faktor propagasi lainnya

- Tidak memperhatikan di bagian perangkat antara User Equipment (UE) pelanggan dan sentral operator UMTS baik itu dari segi *hardware* maupun *software*nya

1.5 Metode Penelitian

Dalam menyelesaikan Tugas Akhir ini penulis akan melakukan metode :

1. Study Literatur dan survey dengan mengumpulkan data melalui buku-buku, jurnal ilmiah yang berkaitan dengan algoritma f8, f9 dan kriptografi algoritma KASUMI
2. Percobaan pada simulasi algoritma f8 dan f9 dengan menjalankan program pada komputer untuk mendapatkan data nilai dari analisa berupa lamanya pemrosesan dan ukuran ataupun kondisi data setelah dilakukan enkripsi yang dibandingkan dengan data sebelum dienkripsi .
3. Metode penghitungan nilai *avalanche effect*nya dan tingkat distribusi keacakan ciphertextnya dengan cara membandingkan besarnya perubahan bit antara inputan dan outputan dari hasil enkripsi dan dekripsi pada simulasi algoritma f8.
4. Analisa pengujian kehandalan algoritma f8 dan f9 terhadap *attack*/serangan.
5. Penyusunan laporan tugas akhir dan kesimpulan akhir

1.6 Sistematika Penulisan

Tugas Akhir ini ditulis dengan sistematika :

BAB I PENDAHULUAN

Berisi tentang Latar Belakang, Perumusan Masalah, Pembatasan Masalah, Metodologi Penyelesaian Masalah serta Sistematika Penulisan.

BAB II DASAR TEORI

Membahas dasar teori yang berhubumgan dengan sistem keamanan UMTS (Universal Mobile Telecommunication System) menggunakan algoritma f8 dan f9. Teori dasar ini difokuskan pada teori-teori dasar pada mekanisme, kriptografi, algoritma KASUMI, algoritma f8 dan f9 itu sendiri.

BAB III PERANCANGAN SIMULASI ALGORITMA f8 DAN f9

Bab ini akan membahas proses perancangan implementasi software algoritma f8 dan f9.

BAB IV HASIL DAN ANALISA

Membahas tentang analisis dari hasil pengujian ataupun percobaan pada simulasi algoritma f8 dan f9.

BAB V KESIMPULAN DAN SARAN

Pada bab ini akan menjelaskan kesimpulan dan saran sebagai hasil dari analisa dan simulasi Tugas Akhir.