1. Pendahuluan

1.1 Latar belakang

Global System for Mobile Communication atau biasa disingkat dengan GSM merupakan standar global komunikasi bergerak digital yang dispesifikasikan oleh *Groupe Speciale Mobile* di Eropa. Sekarang ini, jaringan berbasis GSM digunakan oleh lebih dari 130 negara di dunia. GSM mendukung layanan komunikasi suara dan data yang beroperasi pada frekuensi 900 MHz, 1800 MHz, dan 1900 MHz. Masalah keamanan komunikasi menjadi satu faktor penting yang harus diperhatikan pada jaringan GSM karena medium komunikasi berbasis *wireless* cenderung lebih rentan terhadap berbagai serangan. Salah satu cara untuk menjaga keamanan tersebut adalah dengan menerapkan proses kriptografi. Algoritma yang digunakan untuk mengenkripsi trafik suara dan data *user* antara *mobile station* dan *base station* adalah algoritma A5. Algoritma ini diimplementasikan pada *mobile station* dan *Base Station Subsystem* (BSS).

Algoritma A5 terdiri dari tiga versi yaitu A5/1, A5/2 dan A5/3. Algoritma A5/1 dan A5/2 merupakan algoritma yang umum digunakan pada GSM. Namun, pada tahun 2006 Elad Barkan, Eli Biham dan Nathan Keller telah mendemonstrasikan serangan terhadap A5/1 dan A5/2 di mana penyerang dapat menyadap percakapan melalui *mobile phone* kemudian mendekripsikannya baik secara *real time* atau pun tidak [5]. Sejak 1 Juli 2006, GSM *Association* mengamanatkan kepada GSM *Mobile Phone* untuk tidak menggunakan *cipher* A5/2 lagi [2].

Algoritma A5/3 diperkenalkan oleh GSM *Association* dan 3GPP pada tahun 2002 dengan maksud untuk dijadikan algoritma enkripsi standar pada GSM. Algoritma A5/3 merupakan *stream cipher* yang berdasarkan algoritma Kasumi, yaitu suatu blok *cipher* yang memproduksi sebuah *output* 64-bit dari sebuah *input* 64-bit dengan sebuah kunci 128-bit. Algoritma ini memproduksi dua *keystream* 114-bit yang digunakan untuk enkripsi/dekripsi pada *uplink* dan *downlink*. Algoritma A5/3 ini dikatakan lebih kuat dibandingkan dua versi pendahulunya [13]. Oleh karena itu, pada tugas akhir ini akan dibuat suatu aplikasi yang dapat mensimulasikan algoritma A5/3 dan kemudian menganalisis hasilnya.

1.2 Perumusan masalah

Berdasarkan uraian latar belakang tersebut, maka pada tugas akhir ini dapat dirumuskan masalah sebagai berikut:

1. Bagaimana membuat aplikasi yang dapat mensimulasikan algoritma A5/3 untuk proses kriptografi.
2. Bagaimana menganalisis hasil dari percobaan pada aplikasi tersebut sehingga dapat diukur kemampuan dari algoritma kriptografi A5/3 berdasarkan tingkat *avalanche effect*, waktu proses, dan perubahan besar file.

Selain rumusan masalah, pada tugas akhir ini juga ditetapkan batasan-batasan sebagai berikut:

1. Tidak mengimplementasikan hasil aplikasi dalam bentuk *hardware.*

2. Tidak memperhatikan layanan pengamanan lain yang ada pada jaringan GSM seperti proses otentikasi dan verifikasi dengan menggunakan algoritma kriptografi A3 dan A8.
3. Tidak memperhatikan bagian perangkat baik *software* dan *hardware* yang ada pada jaringan GSM antara *mobile station* dan *Base Transceiver Station* (BTS).

1.3 Tujuan

Adapun tujuan dari tugas akhir ini adalah:
1. Membuat suatu aplikasi untuk simulasi algoritma kriptografi A5/3.
2. Menganalisis kemampuan dari aplikasi algoritma kriptografi A5/3 berdasarkan parameter *avalanche effect,* waktu proses, dan perubahan besar file.

1.4 Metodologi penyelesaian masalah

Metodologi penyelesaian masalah yang akan diterapkan pada tugas akhir ini adalah:
1. Studi literatur
   Mempelajari literatur yang relevan dengan permasalahan yakni spesifikasi algoritma A5/3 dan proses kriptografi pada jaringan GSM. Literatur-literatur yang ada tersebut digunakan untuk membantu dalam membuat aplikasi.
2. Analisis dan perancangan model aplikasi yang akan dibuat.
   Pada tahap ini akan dianalisis apa saja kebutuhan sistem, baik *input, output,* atau pun proses dari Algoritma A5/3 dan akan dimodelkan dengan menggunakan *Data Flow Diagram* (DFD).
3. Implementasi aplikasi
   Pada tahap ini akan diimplementasikan aplikasi yang sesuai dengan spesifikasi sebelumnya ke dalam bahasa pemrograman. Implementasi dilakukan dengan menggunakan DELPHI 7.0.
4. Pengujian pada aplikasi
   Pengujian dilakukan untuk mengetahui proses enkripsi/dekripsi yang ada pada aplikasi dan hasilnya yang akan dianalisis.
5. Analisis hasil percobaan
   Menganalisis semua percobaan yang dilakukan berdasarkan parameter yang telah ditentukan yakni tingkat *avalanche effect* dan waktu proses.
6. Penarikan kesimpulan berdasarkan hasil analisis dan penyusunan laporan.