

BAB I

PENDAHULUAN

Pada bagian ini dikemukakan hal yang melatar belakangi pentingnya dilakukan penelitian, rumusan, dan batasan permasalahan yang dilakukan dalam penelitian, tujuan dan relevansi atau manfaat penelitian terhadap perkembangan solusi dari permasalahan yang diangkat, serta sistematika penulisan dalam laporan tugas akhir ini.

1.1 Latar Belakang

Pengiriman informasi melalui jaringan elektronik dalam penelitian ini adalah *Short Message Service (SMS)* memerlukan suatu proses yang menjamin keamanan dan keutuhan dari informasi yang dikirimkan tersebut. Informasi tersebut harus tetap rahasia selama pengiriman dan harus tetap original pada saat penerimaan di tujuan. Layanan *SMS* diketahui memiliki beberapa kelemahan, yaitu kelemahan terhadap masalah keamanan sistem. Kelemahan itu dikarenakan *SMS* menggunakan standard pengkodean yang universal, *SMS* dibangun dengan sistem bahasa program yang sejenis dengan bahasa program *hardware* seperti komputer dan ponsel dapat menerjemahkan semua data dalam frekuensi tertentu yang terbuka. Hal ini dapat menyebabkan seseorang dapat membaca isi *SMS* yang beredar dengan mudah, karena isi dari *SMS* berupa karakter *text* yang dengan mudah dapat dibaca. Untuk menjamin keamanan dan kerahasiaan informasi, dilakukan proses enkripsi dan dekripsi terhadap informasi yang akan dikirimkan. Enkripsi dilakukan pada saat pengiriman dengan cara mengkonversi informasi asli menjadi informasi sementara sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengkonversi informasi sementara menjadi informasi asli. Jadi informasi yang dikirimkan selama proses pengiriman adalah data informasi sementara, sehingga informasi asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Informasi asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Penelitian utama dalam proses enkripsi dan dekripsi adalah penentuan algoritma yang tepat dan efisien yang digunakan dalam proses enkripsi dan dekripsi tersebut. Pada proses enkripsi dibutuhkan algoritma yang dapat mengenkripsi data secara aman dan pada proses dekripsi dibutuhkan algoritma yang dapat mendekripsi kembali data

tersebut dengan tepat. Untuk keperluan tersebut, diperlukan suatu algoritma untuk menghasilkan kunci yang sangat rahasia yang akan digunakan dalam proses enkripsi dan dekripsi tersebut. Salah satu standar algoritma yang umum digunakan untuk proses enkripsi dan dekripsi data adalah *Advanced Encryption Standard (AES)*.

1.2 Perumusan Masalah

Permasalahan yang dipecahkan kali ini adalah, bagaimana mengaplikasikan algoritma enkripsi *AES* untuk aplikasi *SMS* pada OS Android?

1.3 Tujuan dan Manfaat

Tujuan akhir dari pengerjaan tugas akhir ini adalah:

1. Memberikan standart keamanan pada layanan *SMS* sehingga isi *SMS* tidak dapat di baca dengan mudah oleh orang yang tidak berkepentingan.
2. Mengimplementasikan algoritma enkripsi *AES* dalam aplikasi *SMS* pada *handset Android*.

1.4 Batasan Masalah

Agar tugas akhir ini lebih fokus maka ditetapkan beberapa batasan masalah diantaranya:

1. Aplikasi Hanya bekerja menggunakan algoritma *AES*.
2. Aplikasi Hanya berjalan pada *Operating Sistem Android* minimal ginger bread versi 2.3.
3. Pesan yang dikirimkan hanya berupa teks.
4. Panjang *plaintext* dan *key* yang di inputkan adalah 128bit.

1.5 Metodologi Pengerjaan Tugas Akhir

Pengerjaan Tugas akhir ini menggunakan metodologi sebagai berikut :

1. Studi Pustaka

Proses pengumpulan data dan informasi dengan mencari dan membaca sebagai bahan literatur untuk membantu pemecahan masalah serta mempelajari materi-materi tentang algoritma enkripsi *AES* baik yang didapat melalui internet maupun buku. Data berupa teori pendukung, jurnal dan tutorial.

2. Analisis dan Perancangan sistem

Menganalisis Keperluan apa saja yang nantinya di perlukan dalam membangun aplikasi serta merancang alur dan deskripsi sistem berdasarkan hasil analisa.

3. Implementasi

Pembuatan program berdasarkan alur dan *deskripsi* sistem yang telah di buat. Pada proses ini dilakukan pengimplementasian metode Enkripsi data *AES* untuk melakukan enkripsi pada *SMS*.

4. Testing

Pada tahapan ini adalah melakukan Pengujian serta evaluasi terhadap sistem yang dibuat. Apa bila terjadi kekurangan maka akan dilakukan perbaikan.

5. Penulisan Laporan

Tahap ini merupakan tahap terakhir dari penyusunan tugasakhir. Pada tahap ini dilakukan penulisan laporan dari tugas akhir yang dikerjakan.

1.6 Sistematika Penulisan

Laporan tugas akhir ini di bagi menjadi lima bagian pembahasan yaitu :

BAB I : PENDAHULUAN

Pada bab ini terdiri dari : latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini diuraikan mengenai teori-teori penunjang dalam penulisan buku, diktat, maupun materi dari internet.

BAB III : METODOLOGI PENELITIAN

Berisi secara rinci tentang perancangan sistem dari analisa awal, sistem utama, algoritma, serta analisis perhitungan dalam aplikasi tugas akhir ini.

BAB IV : IMPLEMENTASI

Menjelaskan tentang implementasi program, proses kerja sistem meliputi arsitektur sistem, desain sistem, desain *interface*, dan menguraikan tentang hasil uji coba serta analisis terhadap sistem.

BAB V : PENUTUP

Berisi simpulan yang telah didapatkan dari hasil uji coba sistem dan analisisnya, selanjutnya akan di kemukakan saran-saran mengenai penggunaan sistem serta bahan masukan bagi penyusun bagi rencana pengembangan tugas akhir untuk masa yang akan datang.