

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Beberapa tahun terakhir ini terjadi perkembangan yang pesat pada dunia teknologi, salah satunya pada telepon selular. Penggunaan telepon selular sebagai salah satu media komunikasi dan informasi saat ini menjadi suatu kebutuhan yang cukup penting dan sangat populer. Selain digunakan sebagai media komunikasi suara, telepon selular juga digunakan untuk berkomunikasi lewat layanan *Short Message Services* (SMS). Dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS.

Masalah keamanan merupakan suatu aspek penting dalam pengiriman data maupun informasi melalui layanan SMS. Hal ini disebabkan karena kemajuan di bidang teknologi informasi sehingga memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Hal tersebut dapat mengakibatkan proses pengiriman data menjadi tidak aman dan bisa saja dimanfaatkan oleh orang maupun pihak lain yang tidak bertanggung jawab untuk mengambil data atau pun informasi ditengah pengiriman dan penerimaan. Oleh karena itu, dibutuhkan suatu sistem keamanan yang dapat menjaga kerahasiaan suatu data maupun informasi, sehingga data tersebut dapat dikirim dan diterima dengan aman. Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah dengan teknik pengamanan data yang membuat pesan, data, maupun informasi tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali untuk penerima yang berhak. Teknik pengamanan data menggunakan enkripsi dan dekripsi dikenal dengan nama kriptografi, sebagai sebuah ilmu atau seni untuk mengamankan pesan atau data dengan cara menyamarkan pesan tersebut sehingga hanya dapat dibaca oleh pengirim dan penerima pesan.

Pada tugas akhir ini akan dirancang sebuah aplikasi pengamanan data dalam proses pengiriman dan penerimaan SMS sebagai solusi dari masalah di atas. Perancangan aplikasi ini menggunakan algoritma FEAL dan diimplementasikan menggunakan fasilitas *Wireless Messaging API* (WMA)

dari Java 2 *Micro Edition* (J2ME). Hasil yang diharapkan dari tugas akhir ini adalah mendapatkan hasil enkripsi dan dekripsi dengan performansi yang baik.

1.2 Tujuan Penelitian

Adapun tujuan dari penelitian Tugas Akhir ini adalah:

- a. Merancang aplikasi untuk mengenkripsi SMS sehingga pesan yang dikirim sudah berupa cipher teks yang tidak bisa di baca di operator.
- b. Merancang aplikasi untuk mendekripsi SMS dengan pesan yang diterima dapat dikembalikan ke bentuk plainteks dan dapat dibaca oleh penerima.
- c. Mengetahui performansi aplikasi enkripsi dan dekripsi SMS untuk mengamankan atau menyembunyikan informasi dari pesan yang dikirim dan diterima.

1.3 Rumusan Masalah

Adapun perumusan masalah adalah sebagai berikut:

- a. Bagaimana cara mengimplementasikan algoritma FEAL pada J2ME?
- b. Bagaimana sistem melakukan enkripsi dan dekripsi data pada J2ME?

1.4 Batasan Masalah

Untuk mencapai tujuan dari penelitian ini, permasalahan dibatasi sebagai berikut:

- a. Data yang digunakan berupa text.
- b. Jenis karakter yang digunakan pada proses enkripsi dan dekripsi adalah alphanumerik.
- c. Bahasa pemrograman yang digunakan adalah J2ME.

1.5 Metodologi Penelitian

Metode yang digunakan selama melakukan penyusunan Tugas Akhir antara lain sebagai berikut:

1. Studi Literatur

Mempelajari teori dan konsep kriptografi, algoritma FEAL, serta pengembangan J2ME dari buku referensi, jurnal ilmiah, internet, dan diskusi yang berguna dalam penyusunan tugas akhir ini.

2. Perancangan

Membahas tentang perancangan pengiriman dan penerimaan sms, enkripsi dan dekripsi sms, serta *user interface* yang akan dibangun untuk masalah yang akan dibahas. Perancangan sistem akan menggunakan bahasa pemrograman J2ME.

3. Implementasi dan Pengujian

Pada tahap ini dilakukan implementasi dan pengujian yang menggunakan simulator *Wireless Toolkit* dan dilakukan pengujian keberhasilan terhadap sistem yang dibuat.

4. Pembuatan Laporan

Tahap akhir dari penelitian ini adalah pembuatan laporan tugas akhir dan sidang tugas akhir.

1.6 Sistematika Penulisan

Untuk mempermudah penulisan maka penulis membagi sistematika penulisan ke dalam beberapa bab untuk membahas dan memenuhi pokok permasalahan dalam penulisan skripsi ini. Dalam penulisan skripsi ini penulis membagi penulisan skripsi dalam lima bab, yaitu :

Bab I PENDAHULUAN

Pada bab ini berisi mengenai latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian dan sistematika penulisan tugas akhir.

Bab II DASAR TEORI

Pada bab ini menjelaskan sumber pustaka yang menguraikan tentang teori-teori kriptografi, Algoritma FEAL dan J2ME(Java 2 Micro Edition) secara umum yang mendukung dan mendasari penulisan tugas akhir ini.

Bab III PERANCANGAN

Pada bab ini dibahas mengenai gambaran umum sistem, perancangan sistem enkripsi dan dekripsi, perancangan antarmuka termasuk diantaranya halaman menu utama, menu “Tulis Pesan”, menu “Inbox” dan menu “Keluar”. Perancangan ini berdasarkan mekanisme dan batasan masalah yang digunakan.

Bab IV IMPLEMENTASI DAN PENGUJIAN

Pada bab ini berisi tentang implementasi dan pengujian pada aplikasi enkripsi dan dekripsi sms.

Bab V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dan saran.