

BAB I

PENDAHULUAN

1.1. Latar Belakang

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang. Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyediakan isi informasi (*plaintext*) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi (*encipher*), dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi (*decipher*), disertai dengan menggunakan kunci yang benar. Kata kriptografi sendiri berasal dari bahasa Yunani, yaitu *kryptós* yang berarti tersembunyi, dan *gráphein* yang berarti menulis. Jadi Kriptografi berarti penulisan rahasia.

Salah satu perkembangan teknologi yang berkembang begitu pesat adalah teknologi *wireless*, baik melalui perangkat handphone, PDA dan sebagainya. Teknologi *wireless* ini sendiri sangatlah luas

mencakup bidang-bidang mulai dari radio, televisi, hingga peralatan komunikasi bergerak. Pada saat ini mayoritas penduduk didunia menggunakan teknologi *wireless* sebagai perangkat komunikasi, salah satunya adalah handphone. Perangkat tersebut pada saat ini telah berkembang dengan banyak fitur yang dimilikinya, salah satunya adalah fitur SMS (*Short Message Service*) yang banyak diminati oleh pengguna handphone sebagai cara alternatif lain dalam berkomunikasi disamping karena mudah digunakan juga karena biaya dari penggunaan fitur ini relatif murah.

Oleh karena itu penulis ingin membuat pengamanan pesan yang masuk dan keluar agar apabila ada sebuah pesan yang bersifat privasi atau pribadi pesan tersebut tidak dapat langsung dipahami maknanya oleh orang lain. Aplikasi ini menggunakan algoritma kriptografi *Affine Cipher* dan *One_Time Pad* sebagai teknik kriptografi yang mencaup proses enkripsi dan dekripsi.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah tersebut dapat dibuat suatu rumusan masalah, yaitu:

Mengimplementasikan algoritma *Affine Cipher* dan *One_Time Pad* untuk mengamankan sms dalam mengirim dan menerima pesan yang

bersifat rahasia, dimana informasi atau isi dari pesan tersebut akan tidak mudah diketahui oleh pihak yang tidak berhak.

1.3. Ruang Lingkup

Aplikasi ini mencakup beberapa hal diantaranya :

1. Dibangun dengan menggunakan bahasa pemrograman J2ME.
2. Terdapat menu tulis pesan yang digunakan untuk menuliskan pesan yang nantinya akan dienkripsikan.
3. Terdapat pesan masuk (*inbox*) yang digunakan untuk menyimpan pesan masuk.
4. Terdapat pesan keluar (*outbox*) yang digunakan untuk menyimpan pesan yang telah dikirim/ pesan keluar
5. Metode Enkripsi dan Dekripsi yang digunakan menggunakan dua metode yaitu *Affine Cipher* dan *One_Time Pad*.
6. Aplikasi ini mengenkripsi dan mendekripsikan pesan berupa text (*SMS*).

1.4. Tujuan Penelitian

Adapun tujuan dari pembuatan aplikasi ini adalah :

1. Untuk membangun suatu aplikasi berbasis teknologi *wireless* yang berfungsi untuk mengamankan pesan-pesan yang bersifat privasi pada fitur SMS (*Short Message Service*).
2. Menjaga kerahasiaan pesan yang dikirim maupun diterima pada pesan yang bersifat privasi.