BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Pada era komputerisasi saat ini, teknologi mampu menghasilkan perangkat keras yang mempermudah komunikasi, *smartphone* adalah salah satu dari sekian perangkat keras komunikasi yang sering digunakan. Dalam menjalankan kinerjanya sebagai perangkat keras komunikasi, *smartphone* mempunyai beberapa fungsi seperti *Short Message Service* (SMS) yang telah berkembang dengan sangat pesat dan telah melekat dengan kehidupan masyarakat.

Namun dengan fitur SMS yang telah ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. Permasalahan keamanan data muncul mengingat beberapa fasilitas transaksi dilakukan menggunakan media ini. SMS pada awalnya dirancang untuk komunikasi tidak sinkron dimana konten yang dikirimkan adalah *plaintext.* Proses pengiriman dan penerimaan pesan berbentuk *plaintext* sangat rentan terhadap upaya penyadapan, pencurian, penipuan dan banyak hal lain terhadap suatu informasi.

Karena itu, dibutuhkan suatu cara untuk mengamankan informasi yang sifatnya penting atau rahasia. Dengan melakukan enkripsi terhadap teks SMS, maka tingkat keamanan informasi dari pesan tersebut dapat ditingkatkan, penerapan kriptografi sangat dibutuhkan dalam menjaga kerahasiaan suatu pesan. Kriptografi adalah ilmu untuk menjaga kerahasiaan informasi dari aspek – aspek yang dapat mengancam keamanan suatu informasi dengan metode dan teknik matematika tertentu.

Saat ini, AES (*Advanced Encryption Standard*) digunakan sebagai standar algoritma kriptografi terbaru. Dengan memanfaatkan algoritma AES ini, maka dapat dikembangkan suatu aplikasi SMS yang memungkinkan pengguna untuk mengirimkan pesan singkat dengan enkripsi teks dan dapat melakukan dekripsi terhadap pesan terenkripsi. Berdasarkan uraian latar belakang diatas, penulis mencoba mengimplementasikan algoritma AES (*Advanced Encryption Standard*) mode CBC (*Cipher Block Chaining*) didalam suatu aplikasi perangkat lunak dan sekaligus menjadi bahan penelitian skripsi dengan judul "IMPLEMENTASI ALGORITMA AES MODE CBC UNTUK ENKRIPSI DAN DEKRIPSI PESAN SMS BERBASIS ANDROID".

1.2. Rumusan Masalah

Berdasarkan latar belakang tersebut, maka dapat diambil rumusan masalah sebagai berikut :

- Membuat aplikasi SMS yang memiliki tingkat keamanan tinggi agar terhindar dari penyadapan.

1.3. Ruang Lingkup

Dalam "IMPLEMENTASI ALGORITMA AES MODE CBC UNTUK ENKRIPSI DAN DEKRIPSI PESAN SMS BERBASIS ANDROID" akan dilakukan beberapa batasan masalah sebagai berikut :

1. Aplikasi SMS ini sebatas pengiriman SMS berbentuk *plaintext* dengan enkripsi maupun tidak dengan enkripsi.
2. Aplikasi SMS ini dapat dijalankan pada perangkat *mobile* berplatform Android minimum versi 2.3 (Gingerbread).
3. Proses enkripsi dan dekripsi menggunakan algoritma AES mode CBC.
4. Pengoperasian aplikasi menggunakan kunci simetri, yaitu kunci enkripsi sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm.*
5. Basis bilangan yang digunakan adalah ASCII 256.

6. Pengirim dan penerima pesan menggunakan aplikasi tersebut.
7. Kunci pesan sudah disepakati kedua belah pihak (pengirim dan penerima) secara manual (bertemu) maupun dengan media lain seperti email atau sms biasa.

1.4. Tujuan

Tujuan dalam penelitian ini untuk mengamankan informasi yang sifatnya penting atau rahasia. Dengan melakukan enkripsi terhadap teks SMS, maka tingkat keamanan informasi dari pesan tersebut dapat ditingkatkan.