BAB I

PENDAHULUAN

1.1 Latar Belakang

Beberapa tahun terakhir ini perkembangan teknologi sangatlah pesat. Semakin banyaknya teknologi yang tersebar luas, maka semakin banyak pula masalah-masalah yang terjadi. Telepon seluler merupakan salah satu hasil dari perkembangan teknologi komunikasi. Dengan adanya telepon seluler, maka dapat mempermudah orang untuk saling berkomunikasi antara satu dengan yang lainnya. Terdapat beberapa fungsi yang dapat digunakan dalam telepon seluler antara lain telepon, *Short message service* (SMS), *Multimedia Messaging Service* (MMS), *chatting*, *video call*, internet, dan lain-lain. Di antara beberapan layanan tersebut, SMS menjadi salah satu layanan komunikasi yang paling disukai, hal tesebut di karenakan setiap telepon seluler yang beredar baik mahal maupun murah memiliki layanan SMS. Namun sayangnya SMS tidak dapat menjamin keamanan dari pesan yang disampaikan maupun diterima, hal tersebut terbukti dengan adanya isu penyadapan oleh Australia pada orang nomor satu di Indonesia yang terjadi di tahun 2009. Ada beberapa risiko yang dapat mengancam keamanan pesan pada layanan SMS antara lain SMS *interception* dan SMS *snooping*.

Celah keamanan terbesar pada layanan SMS adalah pada saat SMS tersebut dikirim melalui jaringan Telekomunikasi. SMS bekerja pada jaringan *nirkabel* yang memungkinkan terjadinya pencurian isi pesan SMS ketika dalam proses transmisi dari pengirim ke penerima, hal tersebut merupakan ancaman SMS *interception*.

Ancaman SMS lainnya adalah SMS *snooping*, SMS *snooping* lebih sering terjadi karena kelalaian pengguna telepon seluler. Contohnya ketika seseorang meminjamkan telepon selulernya pada orang lain untuk menggunakan telepon selulernya. Pada saat itu orang tersebut dapat dengan sengaja atau tidak membuka isi pesan yang ada pada *inbox* SMS.

Untuk itu dibutuhkan sebuah sistem keamanan pada layanan SMS yang mampu menjaga integritas dan keamanan isi pesan untuk menutupi celah keamanan SMS (terutama untuk SMS *interception* dan SMS *snooping*). Agar isi pesan hanya bisa dibaca maknanya oleh pengirim dan penerima, isi pesan sebelum dikirim melalui SMS harus dienkripsi terlebih dahulu dengan algoritma kriptografi, misalnya AES dan Vigenere *Cipher*. Penerima dapat membaca makna dari pesan tersebut dengan melakukan dekripsi isi pesan tersebut menggunakan kunci yang sama yang digunakan oleh pengirim. Apabila ada orang lain yang mencuri isi pesan tersebut, orang tersebut tidak akan mampu membaca makna pesan tersebut.

Berdasarkan latar belakang masalah yang ada, maka penulis mengangkat judul "***Penerapan Algoritma AES (Advance Encryption Standard) 128 dan Vigenere Cipher pada Aplikasi Enkripsi Pesan Singkat Berbasis Android***". Diharapkan hasil akhir dari aplikasi ini dapat bermanfaat bagi semua pengguna SMS yang menginginkan keamanan yang lebih.

1.2 Rumusan Masalah

Keamanan data merupakan suatu hal yang harus diperhatikan, apalagi jika data tersebut bersifat rahasia. Berdasarkan uraian latar belakang di atas, penulis mengidentifikasi beberapa hal yang berhubungan dengan masalah keamanan data pada ponsel antara lain :

1. Bagaiman menganalisis cara kerja algoritma AES dan Vigenere *Cipher*?
2. Bagaimana implementasi algoritma AES dan Vigenere *Cipher* pada aplikasi enkripsi pesan singkat berbasis Android?

1.3 Ruang Lingkup

Dalam penulisan tugas akhir ini penulis akan membatasi masalah pada beberapa hal berikut ini :

1. Metode Kriptografi yang digunakan yaitu Algoritma AES (*Advance Encryption Standar*) dan Vigenere *Cipher*.
2. Panjang kunci yang digunakan untuk AES yaitu 128bit.
3. Kunci yang digunakan hanya kunci Simetri
4. Informasi yang akan di enkripsi hanya pesan singkat (SMS) pada ponsel yang berbasis Android.
5. *Hardware* yang digunakan ialah ponsel yang berbasis ANDROID.
6. Versi Android yang *support* minimum 2.2 dan maksimal 4.1.
7. Untuk melakukan penghapusan SMS, harus menggunakan aplikasi SMS bawaan *device* yang digunakan.

8. Pada aplikasi belum bisa menampilkan *Inbox* dalam bentuk *thread*, karena setiap proses pengiriman SMS harus menginputkan *key*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui cara kerja Algoritma AES dan Vigenere *Cipher*.
2. Mengimplementasikan algoritma AES dan Vigenere *Cipher* pada aplikasi pesan singkat berbasis Android.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini ialah sebagai berikut :

1. Membantu pengguna SMS khususnya yang menggunakan perangkat mobile berbasis Android dalam mengamankan konten SMS antar pengirim dan penerima.
2. Terhindar dari ancaman SMS *interception* dan SMS *snooping*.