

## **BAB I**

### **PENDAHULUAN**

#### **1.1 LatarBelakang**

SMS (*Short Message Service*) mulai dikembangkan pada tahun 1991, dan sekarang SMS ini telah diterima secara global sebagai *wireless service* yang memungkinkan transmisi atau pengiriman pesan *alphanumeric* (teks) antar telepon selular. Meskipun SMS dibatasi hanya sampai 160 karakter saja, SMS ini adalah metode komunikasi *non-voice* yang tidak mahal.

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 disini mengingat beberapa fasilitas transaksi dilakukan menggunakan media ini. Bagaimanapun data *plaintext* seperti SMS dapat dicegat di jalan oleh siapa saja yang memiliki akses ke sistem SMS. Server SMS milik operator merupakan salah satu pihak yang dapat mengambil data ini, walaupun dalam setiap perjanjian terdapat klausul tentang kerahasiaan data, akan tetapi data *plaintext* yang terkirim dan

berkasnya tersimpan di berbagai tempat baik di server milik operator maupun milik *content provider* membawa satu potensi bahaya yang besar. Kemudahan dalam bertukar informasi melalui SMS ini disalah gunakan oleh beberapa pihak. Beberapa orang dengan berbagai cara mencoba mencuri informasi yang bukan hak mereka. Hal ini tentunya akan sangat berbahaya untuk pengguna, terutama bagi mereka yang sering mengirimkan data dan informasi rahasia melalui SMS.

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. Metode yang bias digunakan, yaitu gabungan metode Vigenere cipher dan Caesar cipher dengan pengacakan data menjadi *ciphertext* yang mengutamakan keamanan data itu sendiri. Aplikasi SMS ini akan dibangun berbasis *mobile* pada *platform* Android.

## 1.2 Rumusan Masalah

Berdasarkan uraian latar belakang masalah di atas dapat dirumuskan yaitu, bagaimana mengimplementasikan kriptografi metode *Vigenere cipher* dan *Caesar cipher* untuk mengenkripsi data pada layanan SMS.

## 1.3 RuangLingkup

Untuk menjaga focus penelitian, maka ruang lingkup permasalahan mencakup hal-hal sebagai berikut.

1. Metode enkripsi yang diterapkan pada aplikasi dibatasi hanya pada metode *Vigenere cipher* dan *Caesar cipher*.
2. Aplikasi yang akan dibuat hanya dapat digunakan pada system operasi Android.
3. Aplikasi yang akan dibuat hanya dapat mengirimkan data sms berupa data teks yang karakter-karakternya tersedia pada *keyboard* jenis *qwerty* di *mobile phone* berbasis android .

4. Kunci yang digunakan dalam aplikasi ditanam dalam aplikasi sehingga, baik penerima maupun pengirim sms harus memiliki aplikasi yang sama.

#### **1.4 Tujuan penelitian**

Dari perumusan masalah diatas peneliti bertujuan untuk membantu mengamankan suatu transaksi informasi berupa SMS agar tepat sasaran, dan apabila salah tujuan atau dibajak oleh pihak lain maka isi SMS tidak mudah terbaca.