BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era modern sekarang ini perkembangan teknologi semakin pesat, salah satunya adalah telepon selular (ponsel). Mulai dari ponsel yang hanya bisa digunakan untuk bicara dan sms hingga "ponsel cerdas" (*smart phone*) yang memiliki berbagai fungsi seperti *browsing*, *chatting*, *multiplayer games*, transfer data, video *streaming* dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponsel pun bermunculan, diantaranya yang cukup dikenal luas adalah android. Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui *Short Message Service* (SMS). Namun, dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. SMS memiliki banyak kekurangan dari segi keamanan isi pesan, karena layanan SMS masih belum dilengkapi dengan sistem yang menjamin kerahasiaan isi pesan sehingga orang lain tidak dapat mengetahui isi pesan SMS tersebut.

Dalam perkembangan ilmu kriptografi, telah banyak sekali algoritma yang diciptakan untuk menyembunyikan pesan yaitu algoritma kriptografi klasik dan modern. Kriptografi klasik dapat dengan mudah dipecahkan dengan analisis frekuensi atau pun dengan metode kasiski serta metode kerchoff sedangkan Kriptografi modern belum dapat dipecahkan sampai saat ini. Maka dari itu, untuk menjaga keamanannya, pada layanan SMS harus terdapat fitur keamanan isi pesan yakni salah satunya dengan menggunakan kriptografi yang memanfaatkan kunci untuk mendekripsikan sms yang telah di enkripsi. Enkripsi adalah salah satu cara untuk mengamankan sebuah pesan. Dengan menggunakan enkripsi ini diharapkan dapat meningkatkan keamanan pesan data penggunanya. Salah satu Kriptografi klasik yang memiliki kelemahan yakni Vigenere cipher yang dapat di pecahkan dengan menentukan panjang kunci melalui metode Kasiski.

Oleh karena itu, penulis mencoba membuat sebuah aplikasi pengamanan SMS menggunakan metode Vigenere Cipher Substitusi Homofonik dengan Modifikasi Fibonacci untuk mengenkripsi pesan SMS yang berjalan pada sistem operasi android sehingga dapat meningkatkan keamanan terhadap serangan kriptanalis.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah di atas, maka dapat dirumuskan masalah sebagai berikut:

1. Bagaimana menerapkan enkripsi dan dekripsi sms pada handphone yang berbasis android dengan menggunakan metode Vigenere cipher substitusi homofonik yang dimodifikasi dengan fibonacci?
2. Bagaimana penerapan cipher substitusi homofonik pada kriptografi Vigenere cipher yang memodifikasi rumus fibonacci?

1.3 Batasan Masalah

Batasan permasalahan pada penulisan skripsi ini adalah:

1. Perangkat lunak yang di bangun hanya dapat di jalankan pada ponsel yang memiliki sistem operasi android minimal versi 3.0.
2. Dua belah pihak pengguna harus sama-sama menggunakan aplikasi ini.
3. Hanya dapat melakukan pengiriman sms enkripsi dan sms masuk yang dapat di dekripsi.
4. Tidak membahas metode pengiriman kunci.
5. Program yang dibuat merupakan program untuk enkripsi menggunakan karakter – karakter yang ada pada *handphone* kecuali tanda petik (‘) dan garis miring (\).

1.4 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian dan penyusunan skripsi ini antara lain:

1. Membuat aplikasi yang lebih aman untuk pertukaran data (sms) agar privasi pengguna lebih terjamin.

2. Menyembunyikan hubungan statistik antara plainteks dengan cipherteks menggunakan substitusi homofonik.
3. Membangkitkan kunci baru untuk mencegah pengulangan kata pada kunci secara periodik dengan modifikasi pada rumus fibonacci.

1.5 Manfaat Penelitian

1. Bagi Penulis

   Menambah pengetahuan mengenai metode Vigenere cipher substitusi homofonik dengan modifikasi Fibonacci dalam keamanan pesan SMS di android serta mengimplementasikan pengetahuan yang selama ini dipelajari.

2. Bagi Pengguna
   1) Membuat pesan SMS menjadi lebih aman antar pengguna aplikasi ini.
   2) Menanggulangi penyadapan terhadap pesan SMS.