**BAB I**

**PENDAHULUAN**

**1.1 Latar belakang masalah**

Beberapa tahun terakhir ini terjadi perkembangan yang pesat pada teknologi, 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 *multimedia*, *multiplayer games*, *transfer* data, video *streaming* dan lain-lain. Dengan semakin berkembangnya teknologi telepon seluler maka tindak kejahatan pun semakin tinggi diantaranya penyadapan dan pembajakan isi pesan singkat (SMS), Sehingga keamanan perlu dikembangkan agar lebih aman dan handal untuk mengatasinya, karena keamanan telah menjadi aspek yang sangat penting dalam suatu sistem informasi maka salah satu teknik pengamanan yang dapat dipelajari dan dikembangkan terutama untuk pengamanan pesan adalah teknik kriptografi.

Banyak sekali metode kriptografi yang ada, yang dibagi menjadi dua yaitu kriptografi modern dan kriptografi klasik, diantaranya ialah metode stream cipher dan vigenere cipher. Namun pada zaman sekarang ini teknik kriptografi klasik khususnya vigenere cipher tidak dapat menandingi metode metode baru yang lebih baik karena kesederhanaanya, oleh karena itu maka muncul ide untuk membangun system keamana dengan menggunakan metode vigenere cipher yang dikombinasikan dengan stream cipher agar mendapatkan zalgoritma yang kuat.

Dari penjelasan diatas, maka penulis mengangkat menjadi judul skripsi yaitu “PENERAPAN KOMBINASI STREAM CIPHER DAN VIGENERE CIPHER UNTUK SMS MOBILE”. Yang diharapkan dapat membantu pengamanan pesan singkat.

**1.2 Rumusan masalah**

SMS mempunyai beberapa kelemahan seperti pesan yang berupa teks yang sangat mudah dibaca dan dilihat orang, sehingga kerahasiaan dan keamanan saat pengiriman sms sangat diperlukan. Berdasarkan pemilihan judul diatas maka yang menjadi rumusan masalah adalah :

* 1. Bagaimana menerapkan metode kriptografi untuk pengamanan pesan (SMS)
  2. Bagaimana membangun aplikasi untuk mengenkripsi dan deskripsi pesan sebelum dikirim dan dibuka melalui aplikasi sms dengan menggunakan 2 metode yaitu stream cipher dan vigenere cipher.

**1.3 Ruang Lingkup**

Mengingat luas permasalahan yang timbul dan banyaknya aspek dalam membangun suatu aplikasi maka diperlukan ruang lingkup yang jelas untuk menghindari meluasnya pembahasan. Ruang lingkup dalam penelitian ini adalah :

1. Aplikasi ini mengirim dan menerima pesan teks
2. Input yang digunakan pada aplikasi adalah teks
3. Aplikasi ini berjalan apabila pengirim dan penerima pesan telah memiliki aplikasi tersebut
4. Implementasi dari metode ini adalah proses enkripsi dan deskripsi dari data yang diinputkan.
5. Aplikasi ini dikembangkan dengan system operasi windows dan dapat dijalankan pada telepon seluler (HP) yang berpatform JAVA MIDP 2.0

**1.4 Tujuan**

Tujuan dari dibuatnya aplikasi enkripsi sms menggunakan kombinasi stream cipher dan vigenere cipher adalah untuk mengamankan pesan/ informasi berupa data/teks yang dikirim dan diterima dari pihak yang tidak berkepentingan dalam mengakses dan membacanya.