

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Suatu informasi pada jaman global ini makin menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan. Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut tentang aspek-aspek keputusan bisnis, *Privacy*, ataupun kepentingan umum. Dimana informasi-informasi tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya. Semakin berkembangnya dunia teknologi, komunikasi jarak jauh bisa dilakukan dengan saling mengirim email atau data. *Internet* juga telah membuat komunikasi semakin terbuka dan pertukaran informasi juga semakin cepat melewati batas-batas negara dan budaya. Namun tidak semua perkembangan teknologi komunikasi ini memberi dampak yang menguntungkan bagi dunia komunikasi. Penyadapan data merupakan hal yang paling ditakuti oleh pengguna jaringan komunikasi pada saat ini. apalagi data yang dikirimkan adalah pesan yang sangat rahasia. Berbagai usaha dilakukan untuk menjamin agar pesan rahasia yang dikirimkan tersebut tidak bisa diakses oleh pihak lain.

Informasi-informasi rahasia perlu disimpan atau disampaikan melalui suatu cara tertentu agar tidak diketahui oleh pihak yang tidak dikehendaki. Oleh karena itu terciptalah ilmu kriptografi.

Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Pesan yang disamarkan (teks jelas yang dapat dimengerti) dinamakan plainteks, sedangkan pesan hasil penyamaran (teks tersandi) dinamakan chiperteks. Proses kriptografi terdiri atas enkripsi dan dekripsi. Enkripsi merupakan proses penyamaran dari plainteks ke chiperteks sedangkan dekripsi merupakan proses pembalikan dari chiperteks ke plainteks.

Hasil dari enkripsi berupa informasi yang disandikan atau *cipher text*. *Cipher text* dapat diambil informasinya dengan cara membalik sandi tersebut

menggunakan algoritma kriptografi yang sama. Salah satu metode kriptografi adalah *vigenere cipher*.

Berdasarkan uraian latar belakang di atas maka penulis tertarik dengan judul penelitian “Perancangan Aplikasi Keamanan Pesan Teks Dengan Algoritma Kriptografi *Vigenere Cipher*”.

## **1.2 Perumusan Masalah**

Rumusan masalah yang dapat didefinisikan dalam penelitian ini diantaranya adalah sebagai berikut :

1. Bagaimana mendesain proses enkripsi dan proses dekripsi menggunakan Algoritma *Vigenere Cipher*?
2. Bagaimana hasil penerapan algoritma kriptografi *Vigenere Cipher* pada aplikasi keamanan pesan teks?

## **1.3 Tujuan Penelitian**

Penelitian ini bertujuan untuk membangun aplikasi pengamanan data pesan berupa teks dengan teknik kriptografi menggunakan algoritma *Vigenere cipher*, sebagai aplikasi yang mampu melakukan enkripsi dan dekripsi pesan teks .

## **1.4 Manfaat Penelitian**

Manfaat dari penelitian dengan algoritma kriptografi *Vigenere Cipher* dalam keamanan jaringan adalah :

1. Perangkat lunak yang dirancang dapat digunakan sebagai *tools* kriptografi pengamanan data pesan teks dengan metode *Vigenere cipher*.
2. Mengurangi resiko penyalahgunaan hak akses, menyisipkan, menghapus data dari pihak-pihak yang tidak bertanggung jawab.

## **1.5 Batasan Masalah**

Batasan Masalah dari penelitian dengan algoritma kriptografi *Vigenere cipher* dalam keamanan data pesan teks adalah Penelitian ini difokuskan untuk keamanan pesan dengan 65 karakter yaitu penggunaan huruf besar, angka, dan tanda baca pada umumnya.