BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut di kirim dan di terima oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih *authenticity*. Pesan, data, atau informasi akan tidak berguna lagi apabila di tengah jalan informasi itu di sadap atau di bajak oleh orang yang tidak berhak atau berkepentingan.

Keamanan dan kerahasian data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahan, sistem perbankan, sistem bandara udara dan sistem-sistem yang lain setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih di sebabkan karena kemajuan bidang jaringan komputer dengan konsep *open system*-nya sehingga siapapun, di mananpun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka di perlukan beberapa enkripsi guna membuat pesan, data, atau informasi agar tidak dapat di baca atau di mengerti oleh sembarang orang, kecuali untuk penerima yang berhak.

Pengamanan pesan, data, atau informasi tersebut selain bertujuan untuk meningkatkan keamanan, juga berfungsi untuk melindungi pesan, data, atau informasi agar tidak dapat di baca oleh orang-orang yang tidak berhak dan mencegah agar orang-orang yang tidak berhak, menyisipkan atau menghapus pesan, data, atau informasi.

Salah satu hal yang penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin kerahasiaan pesan, data, ataupun informasi adalah enkripsi. Disini enkripsi dapat diartikan sebagai kode atau *chiper*. Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data, atau informasi yang di kirim. Sebuah *chipper* menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (*stream*) bit dari suatu pesan asli (*plaintext*) menjadi *cryptogram* yang tidak di mengerti. Karena sistem *chipper* merupakan suatu sistem yang telah siap untuk di outomasi, maka teknik ini digunakan dalam sistem keamanan jaringan komputer.

Ada banyak model dan metode enkripsi, salah satu di antaranya adalah enkripsi dengan algoritma *Vigenere Chiper*. Di dalam sistem, algoritma ini menjelaskan bagaimana plaintext akan dienkripsi dengan cara pergeseran huruf. Kunci pada kriptografi vigenere adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat secara berulang sepanjang plaintext, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada plaintext.

Berdasarkan uraian di atas, penulis bermaksud untuk mengambil tugas akhir (skripsi) dengan judul "**Aplikasi Algoritma Vigenere Cipher Pada Enkripsi dan Dekripsi Data Teks**".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka dapat dirumuskan permasalahan sebagai berikut :

1. Bagaimana merancang sebuah sistem keamanan data, sehingga data menjadi lebih aman menggunakan Algoritma Vigenere Cipher.
2. Bagaimana menampilkan langkah-langkah penyelesaian metode kriptografi Vigenere Cipher.

1.3 Batasan Masalah

Penelitian ini dibatasi pada permasalahan :

1. Metode yang digunakan pada aplikasi ini adalah metode *Vigenere Cipher* menggunakan Microsoft Visual Basic 6.0.
2. Jenis variable metode vigenere cipher dilakukan terhadap Huruf, Angka & Simbol pada teks.
3. Unit Penyimpanan dan Unit Pembuka File.
   Unit ini digunakan untuk proses penyimpanan data teks yang telah diubah dalam proses enkripsi sehingga menjadi bentuk chipertext dan membuka kembali data teks yang telah disimpan untuk diubah dalam proses dekripsi menjadi data teks asli.

1.4 Tujuan Penelitian

Tugas akhir ini bertujuan untuk :

1. Penelitian ini bertujuan untuk membangun sebuah sistem pengamanan data.
2. Memahami dan mengimplementasikan metode *Vigenere Cipher* ke dalam aplikasi sistem.

1.5 Relevansi

Hasil penelitian ini diharapkan dapat menjadi perangkat lunak atau program yang dapat memberikan keamanan terhadap data, yang nantinya dapat dikembangkan lebih lanjut oleh mahasiswa, dosen atau bagi yang berminat pada sistem keamanan data.