

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Teknologi informasi saat ini banyak membantu pekerjaan di berbagai organisasi maupun pekerjaan pribadi, maka keamanan merupakan suatu aspek yang sangat penting dalam suatu sistem informasi. Sebuah informasi umumnya hanya ditujukan bagi golongan orang tertentu, sehingga sangat penting untuk mencegah jatuhnya data kepada pihak - pihak lain yang tidak berkepentingan agar tidak terjadi kebocoran atau penyalahgunaan data yang dapat dihindari.

Untuk melaksanakan tujuan tersebut, maka dirancang suatu sistem keamanan yang berfungsi melindungi sistem informasi tersebut. Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah kriptografi. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi.

Salah satu aspek keamanan yang perlu dijamin dalam suatu dokumen adalah kerahasiaannya. Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan

demikian informasi hanya akan dapat diakses oleh pihak - pihak yang berhak saja. Dengan begitu memicu banyaknya algoritma kriptografi yang bermunculan sesuai dengan perkembangan zaman.

Berdasarkan semua hal yang telah dijabarkan di atas, maka dalam penyusunan tugas akhir ini, penulis memilih judul "APLIKASI KRIPTOGRAFI MENGGUNAKAN METODE VIGENERE CIPHER DAN ELECTRONIC CODE BOOK (ECB) UNTUK PENGAMANAN DOKUMEN".

1.2. Rumusan Masalah

Permasalahan yang ditangani pada tugas akhir ini adalah :

- a. Bagaimana mengimplementasikan metode kriptografi sebagai pengaman data atau informasi.
- b. Bagaimana membangun aplikasi yang memungkinkan informasi dienkripsi dan dekripsi menggunakan metode *Vigenere Cipher dan Electronic Code Book (ECB)*.
- c. Membangun aplikasi dengan menggunakan bahasa pemrograman *Java Standart Edition (JSE)*.

1.3. Ruang Lingkup

- a. Akan dibangun sebuah perangkat lunak yang dapat mengenkripsi dan mendekripsi menggunakan metode *Vigenere Cipher dan Electronic Code Book (ECB)*.
- b. Aplikasi ini digunakan untuk enkripsi dan dekripsi teks.
- c. Aplikasi ini dapat menampilkan file dengan format txt, doc, docx dan rtf.
- d. Aplikasi ini hanya dapat menampilkan file enkripsi dengan format txt.
- e. Hasil enkripsi berupa *Zip*.
- f. Pembuatan aplikasi ini menggunakan bahasa pemrograman *Java Standart Edition (JSE)*.
- g. Aplikasi ini akan dikembangkan dan dijalankan dalam sistem operasi *Windows*.
- h. Implementasi dari metode ini adalah proses enkripsi dan deskripsi dari data yang diinputkan.

1.4. Tujuan

Tujuan penelitian ini adalah membangun sebuah aplikasi pengamanan data yang berupa teks dengan proses enkripsi dan dekripsi dengan dua metode yaitu metode *Vigenere Cipher dan Electronic Code Book (ECB)*.