BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi informasi dan komputerisasi begitu berkembang pesat saat ini. Seiring dengan perkembangan tersebut, maka memungkinkan dari berbagai lapisan masyarakat, termasuk para cracker dan penjahat lainnya dapat akses keberbagai computer yang diinginkannya. Oleh karenanya kebutuhan akan keamanan kerahasiaan data atau informasi menjadi meningkat pula. Ini semua diperlukan untuk menghindari kejahatan terhadap komputer yang timbul sebagai akibat dari kemajuan teknologi tersebut. Terlebih kalau data tersebut terdistribusi dalam suatu jaringan komputer. Ancaman-ancaman tersebut bisa berupa interupsi, penyadapan, modifikasi maupun fabrikasi.Tentunya ancaman ini akan berakibat pada data-data yang dikomunikasikan.

Dengan berkembangnya ilmu pengetahuan, terutama di bidang informatika, penerapan teknik-teknik pengamanan data yang sudah pernah dipakai jaman dulu bisa menjadi alternatif dalam pengamanan komunikasi data melalui jaringan internet. Sebagai contoh adalah kriptografi, yaitu suatu ilmu dan seni untuk menjaga keamanan pesan yang dikirim dari suatu tempat ke tempat yang lain. Kriptografi sudah dikenal 4000 tahun yang lalu. Kriptografi berkembang pada jaman mesir

kuno dan romawai kuno. Bahkan kriptografi ini memegang peranan penting dalam perang dunia kedua.

Penelitian ini mengimplementasikan algoritma *Electronic Code Book* (*ECB*) yang merupakan salah satu algoritma *private key* dan juga merupakan algoritma *Block Cipher* yang memiliki kemudahan dalam pembentukkan blok-blok bit dan pengiriman blok yang lebih cepat. dan *Caesar Cipher* atau sandi geser, merupakan metode enkripsi yang dilakukan pada zaman Julius Caesar dan merupakan teknik enkripsi paling sederhana dan paling terkenal.

Dengan latar belakang diatas maka peneliti tertarik untuk membuat sebuah sistem pengamanan dengan judul adalah APLIKASI ENKRIPSI DAN DEKRIPSI FILE MENGGUNAKAN KOMBINASI METODE ECB DAN CAESAR CIPHER.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, maka dapat dirumuskan suatu pokok permasalahan yaitu bagaimana membangun aplikasi kriptografi dengan menggunakan metode *ECB* dikombinasikan dengan *Caesar Cipher* yang nantinya mampu melakukan proses mengenkripsi dan mendekripsi suatu pesan dengan menggunakan Bahasa Pemrograman Java.

1.3 Ruang Lingkup

Didalam pengimplementasian kriptografi dengan kombinasi *ECB* dan *Caesar Cipher* ini, ruang lingkup masalah yang akan dibahas meliputi hal-hal sebagai berikut :

1. Proses enkripsi diawali dengan metode *ECB* kemudin *Caesar Cipher* dan pada proses dekripsi diawali dengan metode *Caesar Cipher* kemudian *ECB.*
2. Proses penyandian ASCII 256 *byte*.
3. Aplikasi ini hanya dapat menyimpan dan membuka file teks *.txt dan *.doc.
4. Aplikasi menggunakan kunci *Simetris*
5. Aplikasi yang dibuat ini menggunakan bahasa pemrograman JAVA SE.

1.4 Tujuan Penelitian

Tujuan karya tulis ini adalah untuk membantu mengamankan data atau informasi yang bersifat rahasia agar informasi yang terkandung didalamnya tidak diketahui oleh pihak-pihak yang tidak berkepentingan sehingga memudahkan kelancaran dalam pengiriman informasi.