BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan. Dalam hal ini sangat terkait dengan betapa pentingnya pesan tersebut dikirim dan diterima oleh pihak lain yang berkepentingan, apakah pesan masih asli.

Hal inilah yang menuntut adanya pengamanan terhadap proses pengiriman pesan tersebut sehingga tidak diketahui dan kemudian dimanfaatkan untuk kepentingan pihak ketiga. Telah banyak ditemukan teknik-teknik dalam pengamanan data, salah satunya adalah kriptografi.

Pada umumnya metode kriptografi telah banyak yang diketahui algoritmanya. Dan untuk membuat metode kriptografi yang baru membutuhkan penelitian yang lama. Oleh karena itu salah satu cara termudah untuk dapat mengimplementasikan kriptografi sebagai alat keamanan pesan maka digunakan cara mengkombinasikan metode kriptografi yang sudah ada sebelumnya. Hal tersebut akan memperkuat keamanan dari pesan yang akan dikirim.

Maka peneliti membuat tiga kombinasi metode kriptografi untuk mengamankan pesan.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, maka dapat dirumuskan suatu pokok permasalahan yaitu bagaimana mengimplementasikan kriptografi yang kuat menggunakan metode *Shift Cipher*, *Stream Cipher*, dan *Electronic Code Book* (ECB) yang mampu melakukan proses enkripsi (mengubah pesan asli menjadi sandi) dan dekripsi (mengubah pesan sandi menjadi pesan asli).

1.3 Ruang Lingkup

Ruang lingkup dalam pembuatan aplikasi ini adalah sebagai berikut :

1) Proses enkripsi dan dekripsi dilakukan mengunakan metode *Shift Cipher*, metode *Stream Cipher*, metode ECB dan kombinasinya.
2) Aplikasi ini ditujukan untuk proses enkripsi dan dekripsi terhadap semua format *file*.
3) Kunci yang diinputkan minimal 4 karakter dan maksimal 50 karakter, kecuali pada metode *Shift Cipher* kunci yang

di inputkan hanya 1 karakter dan untuk metode *Stream Cipher* tidak perlu menginputkan kunci.

4) Diimplementasikan menggunakan bahasa pemrograman Java yang berbentuk aplikasi desktop.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma kriptografi yang berisi enkripsi dan dekripsi menggunakan metode *Shift Cipher*, *Stream Cipher*, ECB, dan kombinasi terhadap ketiga metode ini. Implementasi berbentuk 2 aplikasi, yaitu aplikasi enkripsi dan aplikasi dekripsi.