

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan semakin berkembangnya pemanfaatan teknologi informasi, keamanan telah menjadi aspek yang sangat penting dalam suatu sistem informasi. Maka dibangunlah sebuah ilmu mengenai keamanan data yang disebut kriptografi.

Kriptografi adalah ilmu tentang pengaman data, yang berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* yang mengandung arti rahasia (*secret*) dan *graphia* yang mengandung arti tulisan (*writing*).

Dalam sebuah pengamanan data, kriptografi berpengaruh besar dalam pengamanan data khususnya dokumen. Dengan cara isi informasi (*plaintexts*) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi (*ecipher*), dan untuk memperoleh kembali informasi yang asli, dilakukan proses dekripsi (*decipher*), disertai dengan menggunakan kunci yang benar.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan diatas,
yang menjadi rumusan masalah adalah :

1. Bagaimana cara aplikasi tersebut digunakan dalam mengenkripsi dan dekripsi suatu teks.
2. Bagaimana aplikasi tersebut dirancang agar mudah dalam penggunaannya.

1.3 Ruang Lingkup

Agar mudah dijelaskan dalam pembahasan, maka dibuat ruang lingkup yang jelas dalam pembuatan aplikasi ini.

Adapun ruang lingkup tersebut :

1. Aplikasi ini digunakan untuk enkripsi dan dekripsi sebuah teks dengan format extensi .txt
2. Metode enkripsi dan dekripsi teks yang digunakan adalah menggunakan dua metode, yaitu Vigenere Cipher dan Caesar Cipher
3. Aplikasi ini menggunakan tabel ASCII 128 bit
4. Bahasa pemrograman yang digunakan untuk membuat aplikasi tersebut adalah java.

1.4 Tujuan

Membangun aplikasi pengaman file dokumen yang berupa teks dengan proses enkripsi dan deskripsi dengan dua metode yaitu metode Vigenere Cipher dan Caesar Cipher.