BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan dan kerahasiaan data saat melakukan pertukaran informasi merupakan faktor yang sangat penting pada era teknologi informasi dan komunikasi saat ini. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan dan kerahasiaan informasi. Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti dengan teknik kriptografi.

Teknik untuk mengubah informasi yang dapat dibaca/teks asli (*plaintext*) menjadi kode-kode tertentu disebut sebagai enkripsi (*encryption*) dan hasilnya disebut *ciphertext*. Sedangkan teknik untuk mengubah *ciphertext* menjadi *plaintext* disebut dekripsi (*decryption*).

Metode kriptografi dibagi menjadi dua bagian yaitu kriptografi klasik dan kriptografi moderen. Banyak metode yang dapat digunakan. Oleh karena itu, muncul suatu ide untuk membangun sistem keamanan data menggunakan metode *shift cipher* yang dikombinasikan dengan metode *stream cipher* agar mendapatkan suatu algoritma pengamanan data yang kuat.

1.2 Rumusan Masalah

Bagaimana membangun suatu aplikasi kriptografi yang kuat dengan mengkombinasikan metode *shift cipher* dan *stream cipher* untuk melakukan proses enkripsi dan dekripsi suatu data atau informasi.

1.3 Ruang Lingkup

Dalam Penelitian ini mencakup ruang lingkup masalah sebagai berikut :

1. Proses enkripsi dilakukan menggunakan metode *Shift Cipher* kemudian dengan metode *Stream Cipher* dan untuk proses dekripsi dilakukan dengan metode *Stream Cipher* kemudian dengan metode *Shift Cipher*.
2. Enkripsi dan Dekripsi data dilakukan dengan kode ASCII 256.
3. Aplikasi ini mampu melakukan enkripsi dan dekripsi file teks dengan format *.txt dan *.rtf.

1.4 Tujuan

Tujuan penelitian ini adalah untuk membangun sebuah aplikasi enkripsi dan dekripsi data dengan kombinasi metode *shift cipher* dan *stream cipher* untuk menjaga keamanan dan kerahasiaan informasi yang dianggap penting.