BAB I

PENDAHULUAN

1.1 Latar Belakang

Untuk melindungi *file* yang terdapat pada komputer atau tempat penyimpanan data dari akses illegal salah satu caranya adalah dengan menggunakan kriptografi.

Kriptografi juga diperlukan dalam melindungi dokumen dari orang yang tidak berhak untuk merubah isi dokumen, merubah password atau pemanfaatan dokumen tersebut untuk keuntungan pribadi.

Dalam kriptografi terdapat beberapa metode yang cukup penting dalam pengamanan data, untuk menjaga kerahasiaan data salah satunya adalah enkripsi (*encryption*). Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi *chipertext*. Sedangkan suatu proses yang dilakukan untuk mengubah pesan tersembunyi menjadi pesan asli disebut dekripsi. Pesan biasa atau pesan asli disebut *plaintex* sedangkan pesan yang telah diubah atau disandikan supaya tidak mudah dibaca disebut dengan *chipertext*.

Kriptografi akan merahasiakan informasi dengan menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Saat ini banyak bermunculan algoritma kriptografi yang terus dianalisis, dicoba dan disempurnakan untuk mencari algoritma yang dianggap memenuhi standar keamanan. Beberapa algoritma kriptografi yang dikenal antara

lain *DES, Rijndael, Blowfish, RC4, Vigenere Cipher, Enigma, IDEA* dan lainnya.

Blowfish merupakan salah satu algoritma yang tidak dipatenkan dan cukup kuat karena memiliki ruang kunci yang besar dan panjangnya bisa beragam, sehingga tidak mudah diserang pada bagian kuncinya. Suatu sistem kriptografi yang baik terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.

Blowfish pada strategi implementasi yang tepat akan lebih optimal, dapat berjalan pada memori kurang dari 5 KB dan kesederhanaan pada algoritmanya. Untuk itu dibangun sebuah aplikasi yang dapat digunakan untuk mengamankan data atau informasi berupa *file* dengan menggunakan metode *Blowfish* ini. Selain itu diharapkan pula aplikasi yang dibangun ini dapat melihat kinerja algoritma *blowfish* dari segi waktu prosesnya.

1.2 Rumusan Masalah

Rumusan masalah dalam pembuatan dan implementasi aplikasi ini adalah bagaimana mengimplementasi algoritma blowfish dengan kunci asimetris untuk enkripsi dan dekripsi file.

1.3 Ruang Lingkup Penulisan

Dalam pembangunan dan implementasi aplikasi ini, penulis membatasi permasalahan tentang:

a. Merancang aplikasi enkripsi dan dekripsi menggunakan teknik kunci asimetris algoritma *blowfish* dengan objek yang berupa *file text*.

b. Ukuran maksimal *file text* yang digunakan adalah 5 *Megabyte*.

c. Merancang enkripsi dan dekripsi chipertext dengan algoritma RSA.

1.4 Tujuan dan Manfaat Penulisan

1.4.1. Tujuan

Adapun tujuan yang ingin dicapai penulis ini adalah dapat merancang dan mengimplementasikan teknik kunci asimetris algoritma *blowfish* pada aplikasi kriptografi file.

1.4.2. Manfaat

Adapun manfaat dari perancangan dan implementasi aplikasi ini adalah sebagai berikut :

a) Mengamankan dan menjaga kerahasiaan data dengan menggunakan aplikasi kriptografi *blowfish*.

b) Dapat menyamarkan *file input* dan mengembalikannya kembali menjadi *file* semula (enkripsi dan dekripsi dapat bekerja)

c) Sebagai referensi untuk penelitian yang berhubungan dengan algoritma *blowfish* lebih lanjut.

1.5 Sistematika Penulisan

Adapun susunan penulisan laporan ini, penyusunannya diuraikan dalam beberapa bab yaitu sebagai berikut :

BAB I **: PENDAHULUAN**

Berisikan tentang latar belakang, rumusan masalah, ruang lingkup penulisan, tujuan dan manfaat penulisan, dan sistematika penulisan.

BAB II **: LANDASAN TEORI**

Bab ini berisikan hasil penelitian – penelitian yang telah dilakukan dan dasar – dasar teori guna untuk sebagai pedoman, acuan dan penunjang dalam penyelesaian masalah.

BAB III **: METODE PENELITIAN**

Bab ini berisi mengenai metode penelitian yang digunakan dengan menggunakan metode waterfall.

BAB IV **: PERANCANGAN SISTEM**

Bab ini berisi tentang penjelasan mengenai analisis dan desain perancangan dari aplikasi yang dibuat.

BAB V **: HASIL DAN PEMBAHASAN**

Bab ini berisi tentang pengujian sistem, perangkat lunak, dan perangkat keras yang digunakan.

BAB VI **: KESIMPULAN DAN SARAN**

Bab ini berisi kesimpulan dari aplikasi yang dibuat dan saran – saran yang bermanfaat dalam pengembangan aplikasi lebih lanjut.

DAFTAR PUSTAKA

LAMPIRAN