BAB I

PENDAHULUAN

1.1. Latar Belakang

Salah satu hal yang penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin keamanan pesan, data maupun informasi adalah enkripsi. Enkripsi dapat diartikan sebagai kode atau *chipper*. Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data atau informasi yang dikirim. Sebuah *chipper* menggunakan suatu algoritma yang dapat mengkodekan semua aliran data *(stream)* dari suatu pesan asli *(plaintext)* menjadi *cryptogram* yang tidak dimengerti. Sistem *chipper* merupakan suatu sistem yang telah siap untuk dioutomasi, maka teknik ini digunakan dalam sistem keamanan jaringan komputer.

Kriptografi *(Cryptography)* berasal dari bahasa Yunani yaitu *"crypto"*yang berarti rahasia dan *"graphy"*yang berarti tulisan. Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman. Para pelaku kriptografi disebut *cryptographers*. Sebuah algoritma kriptografik *(cryptographic algorithm)* disebut *chipper*, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Kedua persamaan matematik tersebut memiliki hubungan matematis yang cukup erat.

Kriptografi menggunakan suatu algoritma dan kunci untuk mengenkripsi dan mendekripsi data. Algoritma adalah fungsi matematika yang digunakan untuk

mengenkripsi dan mendekripsi data. Oleh sebab itu maka muncul ide untuk membuat aplikasi kriptografi untuk mengamankan data dan juga sebagai implementasi dari sebuah algoritma dalam kriptografi ini yaitu algoritma *SAFER*.

1.2. Rumusan Masalah

Berdasarkan uraian dari latar belakang masalah tersebut di atas maka dapat dirumuskan permasalahan yaitu bagaimana membuat aplikasi kriptografi kerahasiaan data berupa enkripsi dan dekripsi beserta pemecahan pendistribusian kunci.

1.3. Batasan Masalah

Pembuatan tugas akhir ini hanya dibatasi dalam lingkup pemecahan problem pendistribusian kunci dalam enkripsi yaitu algoritma yang nantinya dipergunakan untuk menyelesaikan aplikasi kriptografi ini dan algoritma pembuat kunci dalam hal pengamanan pengiriman pesan yang berupa teks.

1.4. Tujuan Penelitian

Menerapkan ilmu keamananan jaringan komputer dalam kaitannya memecahkan problem pendistribusian kunci beserta algoritma pembuat kuncikedalam aplikasi yang nantinya berguna untuk kemanan data berupa enkripsi dan dekripsi. serta dapat digunakan sebagai referensi pengembangan pembuatan aplikasi kriptografi selanjutnya.

1.5. Manfaat Penelitian

Adapun manfaat yang diperoleh dalam implementasi aplikasi ini adalah sebagai berikut :

1. Membantu mengamankan kerahasiaan data.
2. Dapat dikembangkan menjadi sebuah aplikasi yang nantinya dapat digunakan untuk aplikasi kriptografi yang lain.
3. Memudahkan pemakai untuk membuat kunci pribadi dalam nantinya membuka aplikasi enkripsi dekripsi ini.

1.6. Sistematika Penulisan

Untuk memberikan gambaran yang lebih jelas pada penulisan skripsi ini, maka penulisan dibagi secara sistematis ke dalam lima bab yaitu :

BAB I PENDAHULUAN

Pada bab ini akan dijelaskan latar belakang yang menjadi motivasi dalam melakukan skripsi, rumusan permasalahan yang menjelaskan kondisi sistem yang berjalan saat ini dan permasalahan yang dihadapi dalam lingkungan kerja skripsi, tujuan dan manfaat yang ingin dicapai, rincian pelaksanaan skripsi, dan sistematika penulisan, yang menjelaskan secara singkat dari tiap bab.

BAB II LANDASAN TEORI

Pada bab ini akan dijelaskan teori-teori yang menjadi landasan dalam penyusunan laporan skripsi, yang didasarkan pada topik skripsi yang diambil.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan latar belakang dalam pembuatan sistem. Menganalisis metode yang akan digunakan, serta membuat rancangan *user interface* dan rancangan struktur sistem.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini menjelaskan mengenai implementasi, fitur dan cara kerja sistem serta pengujian *input*, *output*, proses dan koding yang telah dibuat untuk sistem ini.

BAB V PENUTUP

Bab ini berisikan kesimpulan dari penyelesaian masalah, keterbatasan dan rekomendasi untuk pengembangan sistemselanjutnya.