BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Masalah keamanan suatu data menjadi isu penting pada era teknologi informasi saat ini. Pengamanan data tidak hanya sebatas mengupayakan agar data tersebut tidak dibaca oleh pihak yang tidak berkepentingan, tetapi juga bagaimana agar data tersebut tidak dapat dimanipulasi atau dimodifikasi, sehingga dibutuhkan suatu cara agar diperoleh keaslian data sebenarnya. Metode pengamanan data yang dikenal dengan kriptografi adalah suatu metode yang dapat digunakan untuk menjaga kerahasiaan data ,keaslian data, dan keutuhan data. Pada penelitian ini penulis menerapkan Algoritma RC4 sebagai teknik kriptografi yang mencakup proses enkripsi dan dekripsi. Enkripsi adalah proses menyandikan *plaintext* (pesan/data asli) menjadi *ciphertext* (data yang sudah disandikan), dan dekripsi adalah proses mengembalikan *ciphertext* menjadi *plaintext.*

Selain itu terdapat permasalahan yang penting dalam dunia teknologi informasi yaitu bagaimana mengolah data dari informasi-informasi yang semakin besar dan kompleks, sehingga lebih cepat,mudah, aman, dan efisien dalam proses penyimpanannya maupun *transfer* data. Untuk mengatasi masalah tersebut,maka salah satu caranya adalah mengkompres data. Kompresi merupakan pengurangan ukuran suatu berkas

menjadi ukuran yang lebih kecil dari aslinya.Adapun algoritma yang digunakan oleh penulis adalah algoritma *Huffman*. Pokok masalah dari penelitian ini adalah bagaimana caranya agar dapat mengatasi masalah keamanan data dan masalah pengolahan data dari informasi yang semakin besar dan kompleks sehingga menjadi cepat dan efisien dalam proses penyimpanannya maupun ransfer datanya.Dan dari permasalahan tersebut digabungkanlah proses dari keduanya yaitu penggabungan proses algoritma RC4 yang dipakai untuk pengaman dan proses algoritma Huffman yang dipakai untuk pengkompresian data.

1.2 **RUMUSAN MASALAH**

Pengamanan data dengan teknik enkripsi dan dekripsi dikenal begitu banyak ragam algoritmanya, maka dalam penulisan ini akan dibatasi hanya pada penjelasan singkat algoritma dari RC4. Algoritma RC4 merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau input *file* pada satu saat. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang variabel.Algoritma ini tidak harus menunggu sejumlah input *file* tertentu diposes, atau menambahkan *byte* tambahan untuk mengenkrip.

Sedangkan dalam kompresi berkas terdapat beberapa metode, maka dalam penulisan ini dibatasi hanya pada penjelasan singkat tentang algoritma yang digunakan, yaitu algoritma *Huffman* (merupakan algoritma yang dipakai dalam metode *Huffman*). Metode *huffman* adalah suatu teknik kompresi data secara statistik yang bekerja dengan mereduksi panjang kode rata-rata dan menghasilkan kode prefiks yang digunakan untuk mempresentasikan simbol-simbol dari suatu jenis huruf.

1.3 RUANG LINGKUP

Lingkup permasalahan yang diteliti meliputi:

1. Ruang lingkup dalam implementasi Algoritma RC4 ini adalah proses enkripsi dan dekripsi *file* data *ASCII* dan data biner berdasarkan langkah-langkah operasi yang digunakan dalam algoritma tersebut. Maka dalam penerapannya sebuah *file* dapat disandikan dengan proses enkripsi sehingga tidak dapat terbaca lagi. Untuk mengembalikannya dilakukan proses dekripsi

2. Ruang lingkup dalam implementasi Algoritma Huffman ini adalah proses kompresi dan dekompresi file berdasarkan langkah-langkah operasi yang digunakan dalam algoritma tersebut. Maka dalam penerapannya sebuah file dapat dikompres dengan proses kompresi sehingga dapat mengurangi ukuran berkas menjadi ukuran yang lebih kecil. Untuk mengembalikannya dilakukan proses dekompresi.

1.4 TUJUAN PENELITIAN

Tujuan penulisan :

1. Dapat mengimplementasikan algoritma RC4 dalam proses enkripsi dan dekripsi data, dalam hal ini bertujuan untuk membantu para pengelola informasi dalam mengamankan informasi atau data dari pihak yang tidak berkepentingan dengan menggunakan teknik enkripsi, sehingga data yang ada tersebut kerahasiaannya dapat tetap terjaga
2. Dapat mengimplementasikan algoritma Huffman dalam proses kompresi dan dekompresi berkas, dalam hal ini bertujuan untuk membantu para pengelola informasi dalam mengolah informasi atau data menjadi ukuran yang lebih kecil dari aslinya yaitu dengan teknik kompresi.