BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Di era globalisasi dimana segala sesuatu terasa berjalan dengan cepat, kemajuan teknologi semakin memudahkan manusia dalam berkomunikasi dan bertukar informasi. Tetapi kemajuan teknologi juga dapat mengganggu dan merusak komunikasi dan pertukaran informasi tersebut.

Keamanan dan kerahasiaan sebuah data atau informasi dalam komunikasi dan pertukaran informasi sangatlah penting. Seringkali data atau informasi yang penting, dalam komunikasi dan pertukaran informasi kadang tidak sampai kepada penerima atau tidak hanya diterima oleh penerima tetapi juga oleh pihak lain yang melakukan pembajakan atau penyadapan. Hal ini membuat data atau informasi tersebut menjadi tidak berguna lagi dan lebih parahnya lagi kadang data atau informasi tersebut oleh para pembajak digunakan untuk menjatuhkan pihak lain. Oleh karena itu kriptografi sangat dibutuhkan dalam menjaga kerahasiaan data atau informasi.

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu data ataupun informasi. Dalam hal ini sangat terkait dengan betapa pentingnya data atau informasi tersebut dikirim dan diterima oleh pihak atau orang yang berkepentingan, apakah data, atau informasi masih *authenticity*..

Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut

keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahanan, sistem perbankan, sistem bandara udara dan sistem-sistem yang lain setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih di sebabkan karena kemajuan bidang jaringan komputer dengan konsep *open system*-nya sehingga siapapun, dimanapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut.Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka diperlukan beberapa enkripsi guna membuat pesan, data, atau informasi agar tidak dapat di baca atau dimengerti oleh sembarang orang, kecuali untuk penerima yang berhak.[KRI03]

Pengamanan pesan, data, atau informasi tersebut selain bertujuan untuk meningkatkan keamanan, juga berfungsi untuk:

1. Melindungi pesan, data, atau informasi agar tidak dapat di baca oleh orang-orang yang tidak berhak.
2. Mencegah agar orang-orang yang tidak berhak, menyisipkan atau menghapus pesan, data, atau informasi.

Informasi dibagi menjadi dua bagian yaitu informasi yang bersifat pribadi dan informasi yang bersifat umum. Informasi yang bersifat pribadi maksudnya informasi yang terkandung hanya untuk satu orang sedangkan informasi yang bersifat umum yaitu informasi yang dapat diketahui oleh orang banyak. Adapun perjalanan informasi tersebut tidak luput dari gangguan-gangguan pihak yang

tidak berhak. Salah satu ilmu untuk menjaga keamanan dan kerahasiaan data atau informasi yaitu *Kriptografi.*

Algoritma kriptografi pertama kali dikembangkan untuk mengizinkan organisasi tertentu yang ditunjuk untuk mengakses suatu informasi. Pertama kalinya algoritma kriptografi ini digunakan untuk petunjuk dalam perang. Julius Caesar dikenal sebagai orang yang pertama kali telah mengembangkan algoritma kriptografi untuk mengirimkan pesan ke tentaranya. Algoritma kriptografi terdiri dari algoritma *enkripsi (E)* dan algoritma *dekripsi (D)*. Enkripsi adalah proses penguraian/pengacakan informasi yang mana menyandikan dari informasi aslinya agar tidak bisa dibaca atau tidak bisa dilihat. Sedangkan dekripsi adalah proses mengembalikan informasi teracak ke bentuk karakter aslinya. Enkripsi dimaksudkan untuk melindungi informasi agar tidak terlihat oleh orang atau pihak yang tidak berhak. Informasi ini dapat berupa nomor kartu kredit, catatan penting dalam komputer, maupun *password* untuk mengakses sesuatu.

Ada banyak model dan metode enkripsi, salah satu di antaranya adalah enkripsi dengan algoritma *Rivest Code 6* (RC6). Model ini merupakan salah satu algoritma kunci simetris yang berbentuk *block chiper*. Algoritma RC6 merupakan salah satu kandidat *Advanced Encryption Standard* (AES) yang diajukan *RSA Security Laboratories* kepada NIST. Algoritma ini merupakan pengembangan algoritma sebelumnya yaitu RC5 dan telah memenuhi semua kriteria yang diajukan oleh NIST.

1.2 Rumusan Masalah

Bagaimana mengaplikasikan kriptografi ke dalam bentuk program dengan menggunakan algoritma kriptografi RC6 untuk mengenkripsi data schingga suatu data tidak dapat diakses oleh orang yang tidak berhak dan data tersebut terjamin keamanannya.

1.3 Batasan Masalah

Adapun program yang dibuat memiliki batasan-batasan sebagai berikut:

1. Algoritma yang digunakan dalam proses enkripsi / dekripsi file adalah algoritma *Rivest Code 6* (RC6).
2. Perangkat lunak yang digunakan adalah menggunakan program Borland Delphi 6.0
3. Karakter input / output yang dipakai dalam proses enkripsi / dekripsi *text* merupakan kode dalam ASCII sedang untuk proses enkripsi pada file yaitu file untuk semua jenis ekstensi dan hasilnya berektensi *.cry

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mempelajari dan memahami kriptografi
2. Memahami dan mempelajari algoritma RC6 dalam mengenkripsi dan mendekripsi file.
3. Menerapkan algoritma RC6 ke dalam bentuk program untuk mengenkripsi dan mendekripsi file.

1.5 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini adalah:

1. Perusahaan atau instansi yang mempunyai data yang sifatnya rahasia tidak dapat dibaca oleh orang yang tidak berhak.
2. Memberikan masukan kepada *user* lain yang mempunyai data baik dalam sekala kecil maupun besar agar data yang disimpan menjadi lebih aman.
3. Dapat mengetahui kinerja algoritma RC6 dalam mengenkripsi dan mendekripsi file.
4. Mengetahui pentingnya memahami kriptografi

1.6 Metode Penelitian

1. Pengumpulan Data
   a. Metode Wawancara, melakukan tanya jawab dengan sumber atau ahli yang mengerti dan memahami masalah untuk mendapatkan data-data yang dibutuhkan.
   b. Metode Pustaka, pengumpulan data yang berhubungan dengan masalah yang diambil, yang bersumber dari buku-buku literatur dan referensi-referensi dari internet.
2. Pembuatan Sistem
   a. Analisis Sistem

      Analisis ini dilakukan untuk mengelola data yang sudah didapat dan mengelompokkan data sesuai dengan kebutuhan perancangan, sehingga dapat menghasilkan sistem yang baik.

b. Perancangan Sistem

Perancangan perangkat lunak dari analisis sistem yang telah dilakukan menggunakan diagram alir (*flowchart*).

c. Implementasi

Penerjemahan hasil rancangan kedalam bahasa pemrograman komputer yaitu menggunakan Borland Delphi 6.0

d. Pengujian Sistem

Tahap ini dilakukan untuk mengetahui bagaimana jalannya sistem apakah sudah berjalan dengan normal atau tidak.

1.7 *Review* Penulisan Sejenis

Pada penelitian yang penulis lakukan ini adalah proses pembelajaran dan menerapkan teknik kriptografi dengan menggunakan algoritma RC6 yang berbentuk *block cipher* untuk keamanan file. Adapun penelitian yang lain yang pernah dilakukan antara lain :

1. Anton Nugroho Irawan yang berjudul Studi dan Implementasi Algoritma *Blowfish* untuk Keamanan *File* adalah menerapkan teknik kriptografi dengan menggunakan algoritma *Blowfish* yang berbentuk *block cipher*.
2. Dian Wahyudi yang berjudul Implementasi Enkripsi / Deskripsi Data Pada *File*, *Text* dengan Menggunakan Algoritma *Rivest Code 4* (RC4), yang berbentuk *stream chiper*.

3. Dan yang sedang dilaksanakan oleh saudara Fikri adalah penerapan kriptografi dengan menggunakan algoritma *Rijndael* yang telah menjadi standart AES dan berbentuk *block chipper*.

1.8 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini merupakan pengantar terhadap permasalahan yang akan dibahas. Di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang masalah, batasan masalah, tujuan penelitian, metode penelitian, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini akan di jelaskan landasan teori, yaitu konsep kriptografi untuk enkripsi dan dekripsi file, dan konsep algoritma yang dipakai yaitu menggunakan RC6 dalam mengenkripsi dan mendekripsi file.

BAB III ANALISIS KEBUTUHAN PERANGKAT LUNAK

Berisi penjelasan mengenai analisis kebutuhan perangkat lunak yang meliputi metode analisis, analisis kebutuhan berupa *input, output* serta antarmuka yang diinginkan.

BAB IV PERANCANGAN PERANGKAT LUNAK

Pada bab ini menjelaskan tentang perancangan yang digunakan dalam metode algoritma RC6. Dengan menggunakan diagram alir untuk menjelaskan enkripsi dan dekripsi file.

BAB V IMPLEMENTASI PERANGKAT LUNAK

Bagian ini memuat batasan implementasi perangkat lunak, implementasi perangkat lunak secara umum, lingkungan pengembangan, bahasa pemrograman yang digunakan, implementasi antarmuka (*interface*).

BAB VI ANALISIS KINERJA PERANGKAT LUNAK

Menganalisis kinerja perangkat lunak sehingga tingkat kesalahan baik dalam pengolahan data maupun dari sistem itu sendiri diharapkan menjadi lebih baik.

BAB VII SIMPULAN DAN SARAN

Bab ini tentang kesimpulan dan saran bagi penulis untuk kesempurnaan program.