BAB I

PENDAHULUAN

1.1. Latar Belakang

Dengan berkembangnya teknologi informasi, pertukaran data dan informasi baik melalui jaringan komputer global maupun orang per orang dengan PC-nya, yang digunakan juga oleh perusahaan yang berskala menengah maupun berskala besar, menyebabkan kecenderungan pemakai jasa layanan internet terus meningkat. Dan ini merupakan fenomena yang harus dicermati oleh pengguna jasa layanan tersebut.

Pemakaian media Internet (*Global Network*) tidak hanya dilakukan oleh orang per-orang melalui PC-nya namun banyak juga digunakan oleh institusi-institusi, agen rahasia negara terutama tentang kekuatan militer atau teknologi persenjataan sangat memberi keuntungan dalam mempercepat lalu lintas data dan informasi ke berbagai tempat di dunia dengan menembus batas ruang dan waktu dengan biaya yang relatif cukup murah.

Masalah yang banyak dibicarakan dalam jaringan global adalah bagaimana memberikan keamanan terhadap data dan informasi karena menyangkut kepentingan pribadi, institusi, keamanan negara dan perusahaan. Oleh karena itu banyak negara-negara maju yang telah menghabiskan dana berjuta-juta untuk menangani dengan serius keamanan komunikasi yang sangat rahasia, terutama yang menyangkut informasi tentang kekuatan agen rahasia negara atau hal-hal yang menyangkut rahasia orang per orang yang melakukan

aktifitas di jaringan komputer global. Oleh karena itu perlu adanya metode yang dapat memberikan keamanan terhadap data dan informasi dari kebocoran terhadap orang lain yang tidak mempunyai wewenang untuk mengetahuinya.

Salah satu metode yang digunakan untuk mengamankan data dan informasi dari tindakan orang yang tidak berwenang untuk mengetahui informasi tersebut adalah metode enkripsi (kriptografi).

Dalam Tugas Akhir ini akan dibahas tentang kriptografi yang digunakan untuk mengamankan data digital dengan metode DES (Data Encryption Standard).

Kriptosistem penting bagi organisasi yang besar seperti pemerintah atau militer juga keperluan individu. Sebagai contoh, jika nomor kartu kredit dikirimkan lewat jaringan komputer, diharapkan nomor tersebut hanya dibaca oleh penerima yang diharapkan.

1.2. Perumusan dan Pembatasan Masalah

Dalam Tugas Akhir ini, masalah yang akan dibahas adalah :

1. Penerapan kriptografi pada sistem keamanan data digital
2. Bagaimana penerapkan metode DES untuk mengenkripsi data digital tersebut

1.3. Tujuan

Laporan Tugas Akhir yang akan ditulis ini memiliki beberapa tujuan yaitu :

1. Bagaimana memahami kriptografi dan hubungannnya dengan keamanan data (*security*), dengan menjelaskan tentang apa dan bagaimana kriptografi jika diterapkan untuk keamanan data digital
2. Setelah memahami point satu selanjutnya akan dipilih dan dianalisa terhadap salah satu metode yang ada dalam kriptografi yaitu metode DES
3. Hasil analisa yang diperoleh dari metode tersebut akan diimplementasikan dengan menyusun program aplikasi sederhana berbasis PCDes Version 1.02 desain dari Greg Carter dan menggunakan bahasa pemrograman Borland Delphi 3.0

1.4. Sistematika Penulisan

Sistematika penulisan Laporan Tugas Akhir yang dibuat oleh penulis adalah sebagai berikut :

Bab I. Pendahuluan

Pada bab ini akan dijelaskan tentang latar belakang penulisan, tujuan, permasalahan dan pembatasannya serta sistematika penulisan laporan tugas akhir ini.

Bab II. Materi Penunjang

Bab ini menerangkan tentang teori penunjang diantaranya teori aljabar (fungsi), teori bilangan (*number theory*) dan lain-lain.

Bab III. Penerapan Kriptografi untuk Keamanan Data

Bab ini akan menjelaskan tentang kriptografi, analisa metode DES dan algoritmanya serta implementasi metode tersebut dalam proses enkripsi atau dekripsi terhadap data digital.

Penutup

Bab ini berisi kesimpulan berdasarkan penjelasan pada bab-bab sebelumnya.