BAB I

PENDAHULUAN

1.1. Latar Belakang

Dengan perkembangan teknologi informasi yang begitu cepat, pertukaran data dan informasi baik melalui jaringan komputer global maupun orang per orang dengan PC-nya menjadi kebutuhan bagi setiap orang agar tidak tertinggal dalam memperoleh informasi. Pemakaian media Internet (Global Network) yang banyak 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.

Sejalan dengan itu muncul pula masalah bagaimana memberikan keamanan terhadap data dan informasi yang dibicarakan, karena menyangkut kepentingan pribadi, institusi, keamanan negara dan perusahaan. Oleh karena itu banyak negara-negara maju yang telah menghabiskan berjuta-juta dollar 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. Untuk 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 cara yang digunakan untuk mengamankan data dan informasi dari tindakan orang yang tidak

berwenang untuk mengetahui informasi tersebut adalah dengan menyandikan informasi tersebut.

Cabang ilmu pengetahuan yang mempelajari penyandian adalah *kriptologi*, kriptologi terdiri dari dua bagian yaitu *kriptografi* dan *kriptaanalis*. Kriptografi adalah seni untuk mengamankan informasi atau plainteks dengan menggunakan tehnik penyandian sedangkan kriptaanalis adalah seni untuk memecahkan sandi. Dalam kriptografi terdapat sistem kriptografi yang disebut *kriptosistem* yang melibatkan dua pihak yaitu pihak pengirim dan penerima. Pengirim akan mengubah informasi asli (*plainteks*) sebelum mengirimkan kepada penerima. Proses penyandian informasi disebut enkripsi sedangkan informasi yang diperoleh dari proses enkripsi disebut *cipherteks*. Kemudian penerima akan menguraikan cipherteks untuk mendapatkan kembali informasi asli (*plainteks*), proses tersebut disebut *dekripsi*.

Dalam Tugas Akhir ini akan dibahas tentang kriptografi yang digunakan untuk mengamankan data digital berupa file text dengan metode GOST (*Gosudarstvenny Standard*). Metode GOST merupakan salah satu metode dalam kriptografi dan dapat dimanfaatkan untuk mengamankan data dengan menggunakan berbagai bahasa pemograman.

1.2. Perumusan Masalah

Dalam Tugas Akhir ini, masalah yang akan dibahas adalah :

1. Kriptografi pada sistem keamanan data digital berupa file text.
2. Implementasi metode kriptografi yaitu Metode GOST menggunakan bahasa pemrograman Delphi.

1.3. Pembatasan Masalah

Implementasi metode GOST (*Gosudarstvennyi Standard*) terhadap data digital tersebut akan dibatasi pada data digital berupa file text serta dimaksudkan hanya pada proses penyimpanan.

1.4. Tujuan

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

1. Memahami salah satu metode yang ada dalam kriptografi yaitu metode GOST.
2. Mengimplementasikan metode GOST dalam membuat program aplikasi sederhana dengan menggunakan bahasa pemrograman Delphi.
3. Aplikasi berupa program yang dibuat tersebut dimanfaatkan untuk mengamankan data pada tingkat penyimpanan (*storage*), yang berarti secara teknis data yang sudah dienkripsi telah aman dari pihak yang tidak mempunyai wewenang untuk mengetahui data tersebut

1.5. Sistematika Penulisan

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

Bab I Pendahuluan

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

Bab II Materi Penunjang

Bab ini menerangkan tentang teori penunjang diantaranya fungsi, teori bilangan dan penjelasan tentang file.

Bab III Penerapan Metode GOST Untuk Keamanan Data Digital

Bab ini akan menjelaskan tentang Kriptografi, metode GOST serta implementasi metode tersebut dalam proses enkripsi atau dekripsi terhadap data digital berupa file text.

Bab IV Kesimpulan

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