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 bersekala 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 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. 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).

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.

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

1.2. PERUMUSAN MASALAH

Dalam Tugas Akhir ini, masalah yang akan dibahas adalah penerapan kriptografi pada sistem keamanan data digital dengan metode IDEA, serta implementasinya terhadap data berupa file text dengan bahasa pemrograman Delphi.

1.3. PEMBATASAN MASALAH

Implementasi metode IDEA terhadap data digital tersebut akan dibatasi pada data digital berupa file text serta dimaksudkan hanya pada proses penyimpanan.

1.4. TUJUAN

Laporan TA yang akan ditulis ini memiliki beberapa tujuan yaitu :

1. Memahami kriptografi khususnya metode IDEA untuk keamanan data digital
2. Mengimplementasikan metode IDEA dengan menyusun aplikasi sederhana, menggunakan bahasa pemrograman Delphi.

1.5. METODE PEMBAHASAN

Alur pembahasan dalam laporan tugas akhir ini akan disusun berdasarkan sistematika penulisan Laporan Tugas Akhir yang tercantum setelah garis besar pemecahan masalah, yang secara ringkas disusun meliputi bab pendahuluan, teori penunjang, penjelasan kriptografi dan analisis terhadap salah satu metodenya yaitu IDEA dan akan ditutup dengan kesimpulan.

1.6. GARIS BESAR PEMECAHAAN MASALAH

1.6.1. PENGANTAR KRIPTOGRAFI

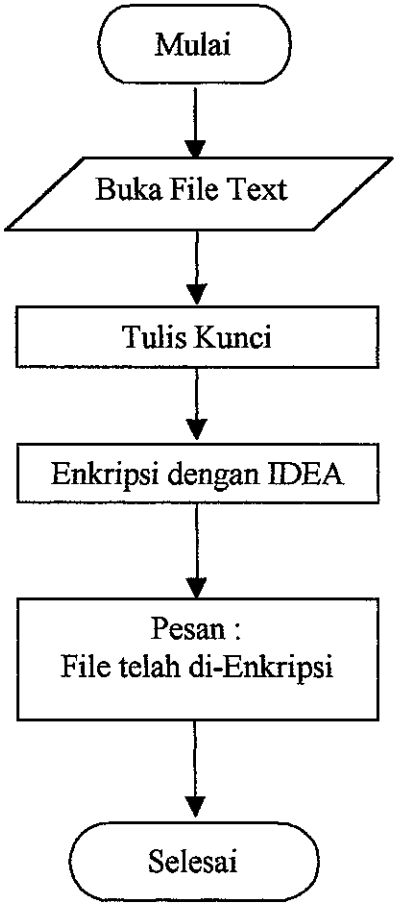
Kriptografi (cryptography) adalah kajian/studi tentang teknik-teknik bersifat matematis yang berkaitan dengan aspek keamanan data atau informasi. Dalam kriptografi digunakan metode atau sistem, yang disebut *kriptosistem (cryptosystem*). Di dalam sebuah kriptosistem, *pengirim (sender*) mengubah pesan sebelum mengirimkannya, sehingga diharapkan hanya penerima *(receiver)* yang berhak untuk bisa menyusun ulang pesan yang asli yakni *pesan yang belum diubah (plaintext atau cleartext).* Kegiatan pengirim pesan ini disebut menyandikan atau *mengkriptosasi (encrypt)* pesan, sedangkan pesan yang terenkripsi disebut *ciphertext* dan penerima pesan dikatakan melakukan

penguraian sandi atau *dekriptografi (decrypt)* pesan. Jika kriptosistem ini aman, orang-orang yang tidak berhak tidak akan bisa menemukan teknik dekripsi, sehingga meskipun mereka membaca pesan yang telah dikriptosasi, mereka tidak akan bisa melakukan dekriptosasi pesan itu.

Kriptografi dilakukan oleh seorang kriptografer (*cryptographers*), sedangkan kripta analis (*cryptanalysis*) adalah kajian/studi terhadap teknik-teknik untuk memecahkan atau membongkar metode kriptografi.

Pada salah satu sistem tertua dan paling sederhana, pengirim dan penerima masing-masing mempunyai sebuah kunci yang mendefinisikan sebuah karakter pengganti untuk setiap karakter potensial yang dikirimkan. Lagipula, pengirim dan penerima tidak memperlihatkan kuncinya. Kunci seperti itu dikatakan kunci private.

Adapun secara umum program yang akan dibuat mengikuti diagram alur berikut ini :



Gambar 1.1. Diagram Alur Proses Enkripsi (analog untuk proses dekripsi)

Plaintext dinotasikan dengan M (*Message*) atau P (*Plaintext*), plaintext berupa text. M secara sederhana adalah data biner. Ciphertext dinotasikan dengan C yang juga merupakan data biner. Fungsi enkripsi E, mengoperasikan M (sebagai input) sehingga diperoleh C, secara matematis dapat dinotasikan sebagai berikut :

$$E(M) = C$$

Sedangkan kebalikannya adalah fungsi dekripsi :

$$D(C) = M$$

Karena proses enkripsi dan dekripsi adalah untuk memperoleh kembali (*recover*) original plaintext, maka harus memenuhi identitas berikut :

$$D(E(M)) = M$$

Kriptografi menyelesaikan masalah ini dengan sebuah kunci (*key*), dinotasikan dengan K. Kunci ini dapat berupa nilai bilangan yang cukup besar. Range dari nilai kunci yang mungkin tersebut disebut Ruang Kunci (*keyspace*). Baik proses enkripsi maupun dekripsi menggunakan kunci tersebut sehingga fungsi diatas menjadi :

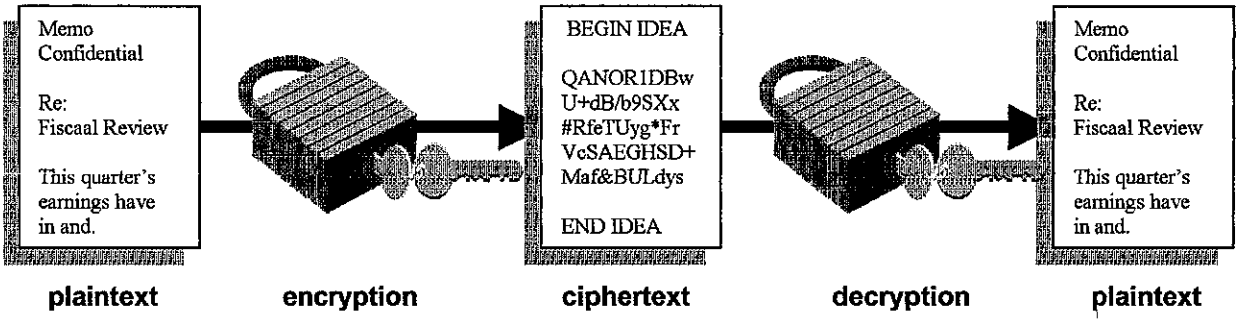
$$E_k(M) = C$$

$$D_k(C) = M$$

Fungsi ini memiliki sifat yang sama dengan yang sebelumnya yaitu :

$$D_k(E_k(M)) = M$$

Proses enkripsi dan dekripsi memakai kunci dapat digambarkan sebagai berikut :



Gambar 1.2. Proses Enkripsi dan Dekripsi dengan Kunci

Teknik enkripsi terbagi atas dua tipe yaitu *enkripsi kunci simetrik* dan *enkripsi kunci publik.* Dan untuk enkripsi kunci simetrik terdapat dua kelas enkripsi yaitu sandi blok (*Block Cipher*) dan sandi berurut (*Stream Cipher).*

Sandi blok adalah skema enkripsi yang membagi pesan plantext menjadi string-string dengan ukuran panjang yang tetap (misalkan *t* disebut blok dari alpabet) serta mengenkripsi satu blok dalam satu waktu.

Sandi berurut adalah skema enkripsi terhadap pesan plantext $(m_1,m_2,m_3...)$ dan menghasilkan sandi $c_1,c_2,c_3,...$ dengan aturan $c_i=Ee_i(m_i)$. Jadi prosesnya pada panjang blok sama dengan satu dengan ruang kunci (*keystream)* untuk transformasi enkripsinya.

1.6.2. METODE IDEA

IDEA merupakan chiper yang berupa blok, mengolah 64 bit blok plaintext. Panjang kuncinya 128 bit. Algoritma yang sama digunakan untuk enkripsi dan dekripsi.

Seperti chiper blok lainnya, rancangan filosofis dibalik algoritma adalah pengoperasian gabungan kelompok aljabar yang berbeda. Tiga kelompok aljabar digabungkan dan diimplementasikan pada hardware dan software, diantaranya:

- XOR
- penjumlahan dengan modulo 2^{16}
- perkalian dengan modulo $2^{16} + 1$

Plaintext dinotasikan dengan M (*Message*) atau P (*Plaintext*), plaintext dapat berupa file text, gambar video digital yang berkaitan dengan komputer dan merupakan data biner. Ciphertext dinotasikan dengan C yang juga merupakan data biner.

1.7. 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) dan teori bilangan (Number Theory) dan lain-lain.

Bab III. Penerapan Metode IDEA untuk Keamanan Dokumen Data Digital

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

Bab IV. Penutup

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