IMPLEMENTASI TEKNIK KRIPTOGRAFI DALAM PENGAMANAN DATA MENGGUNAKAN BAHASA PEMOGRAMAN VB 6.0

TUGAS AKHIR

Diajukan sebagai salah satu syarat
untuk memperoleh gelar Ahli Madya

Oleh :

NUR AFLINA BOER
05 085 038

Program Studi Teknik Telekomunikasi Multimedia
Jurusan Teknik Elektro

POLITEKNIK UNIVERSITAS ANDALAS PADANG

2008

ABSTRAK

IMPLEMENTASI TEKNIK KRIPTOGRAFI DALAM PENGAMANAN DATA MENGGUNAKAN BAHASA PEMOGRAMAN V.B 6.0

Oleh

NUR AFLINA BOER

05 085 038

Keamanan telah menjadi aspek yang sangat penting dari suatu sistem informasi. Sebuah informasi umumnya hanya ditujukan bagi segolongan tertentu. Oleh karena itu sangat penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan. Penerapan kriptografi dapat digunakan untuk mengamankan data. Oleh karena itu, pengguna sistem teknologi informatika membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya

Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, otentikasi, dan ketiadaan penyangkalan. Perancangan program kriptografi dalam pengamanan data ini menggunakan software Visual Basic 6.0.

Kata kunci : Algoritma Kriptografi, Enkripsi, Dekripsi

BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi informasi, keamanan informasi menjadi bahan pembicaraan bagi banyak kalangan diantaranya pemerintah, bisnis komersial dan individu. Mereka menjadikan media ini sebagai aset yang berharga. Namun dengan terjadinya revolusi elektronik maka informasi menghadapi masalah yang serius yaitu keamanan informasi pada proses komunikasi.

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

Pada zaman modern ini, kerahasiaan merupakan hal yang sudah menjadi tuntutan publik yang mutlak. Setiap individu pasti memiliki informasi-informasi pribadi yang ingin disembunyikan agar tidak diketahui oleh pihak-pihak yang tidak berhak. Di bidang komunikasi kerahasiaan dalam penyampaian pesan juga diinginkan oleh semua individu. Apabila seseorang ingin menyampaikan sesuatu pesan yang bersifat pribadi kepada orang lain yang dipercayainya, tentunya orang tersebut tidak menginginkan adanya pihak ke-tiga yang mendapat pesan tersebut. Oleh karena tuntutan-tuntutan seperti itulah ilmu kriptorafi ada dan berkembang. Salah satu cara yang dapat dilakukan untuk mengamankan sistem data adalah dengan kriptografi.

Pada dasarnya, konsep kriptografi mengacu pada proses enkripsi dan dekripsi. Proses enkripsi adalah proses penyamaran dari *plaintext* (teks jelas yang dapat dimengerti) menjadi *ciphertext* (teks tersandi). Sedangkan dekripsi adalah proses pembalikan *ciphertext* menjadi *plaintext* asal.

Kriptografi adalah bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi (*encrypt*) maupun dekripsi *(decrypt*) data. Teknik ini digunakan untuk merubah data ke dalam kode-kode tertentu sehingga informasi yang disimpan atau ditransmisikan melalui jaringan yang tidak aman (misalnya saja internet) tidak dapat diketahui oleh siapapun kecuali oleh orang-orang yang berhak.

1.2 Maksud dan Tujuan

a. Mengamankan dan melindungi data baik teks, gambar, suara maupun video agar tidak dapat dibuka ataupun dirubah oleh pihak lain.
b. Menjamin keaslian suatu pesan.
c. Mengimplementasikan algoritma *Diffie Hillman* yang digunakan untuk mengamankan data.

1.3 Perumusan Masalah

a. Dalam kriptografi terdapat berbagai macam sistem sandi (*Cryptosistem*) yang memiliki algoritma, tujuan penggunaan dan tingkat kerahasiaan yang berbeda. Dalam prakteknya, menentukan algoritma kriptografi yang digunakan menjadi suatu masalah tersendiri.

BAB V
PENUTUP

5.1 Kesimpulan

Dari semua proses pembuatan tugas akhir ini dapat diambil kesimpulan sebagai berikut :

1. Dalam melakukan proses dekripsi, penggunaan *password* harus sama dengan proses enkripsi , supaya proses dekripsi dapat dilakukan dengan baik.
2. Lama waktu yang digunakan dalam proses *encrypt* dan *decrypt* tergantung pada ukuran *file* dan panjang kunci yang digunakan.

5.2 Saran

1. Untuk *password* atau kunci, sebaiknya dipilih sesuatu yang unik, mudah diingat dan bersifat pribadi. Hindari *password* yang berasal dari literatur yang bersifat umum karena akan memiliki kemungkinan yang besar untuk ditebak.
2. Teknologi yang semakin canggih akan membuat seorang kriptanalis semakin mudah mengetahui algoritma yang digunakan oleh orang lain, maka untuk perkembangan berikutnya diharapkan algoritma yang digunakan lebih sulit dipecahkan dan lebih baik dari sebelumnya.