PENYANDIAN DATA DENGAN ALGORITMA KRIPTOGRAFI RSA

SKRIPSI SARJANA MATEMATIKA

Oleh

Mona Elviyenti
03 134 010

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS ANDALAS
PADANG
2007

ABSTRAK

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi-informasi penting dari pihak yang tidak berhak. Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyandikan isi informasi (*plainteks*) menjadi isi yang tidak dipahami (*chipertext*) melalui proses enkripsi, dan untuk memperoleh kembali informasi yang asli dilakukan proses dekripsi, disertai dengan menggunakan kunci yang benar. Langkah-langkah untuk menyandikan isi informasi tersebut disebut Algoritma Kriptografi, salah satunya adalah Algoritma Kriptografi RSA *(Rivest Shamir Adleman)*.

Algoritma Kriptografi RSA yang buat oleh Ron Rivest, Adi Shamir, dan Leonard Adleman ini dapat diaplikasikan ke dalam bahasa program. Program yang digunakan adalah *compiler* Borland Delphi 6.0. Tujuan aplikasi ini adalah untuk melihat cara kerja Algoritma RSA dan untuk melihat perubahan informasi setelah dienkripsi dan didekripsi.

Kata Kunci : *kriptografi, enkripsi, dekripsi, kriptografi RSA, borland delphi 6.0*

BAB 1

PENDAHULUAN

1.1. Latar Belakang Masalah

Saat ini komputer hampir dapat dijumpai di setiap kantor pemerintah, perusahaan, sekolah, atau bahkan rumah tangga. Perkembangan teknologi komputer yang pesat, khususnya di bidang perangkat lunak, membuat komputer menjadi semakin *user friendly* dan telah menjadikannya suatu kebutuhan bagi kalangan tertentu, misalnya kalangan bisnis, pekerjaan yang mereka lakukan sangat tergantung pada komputer. Komputer tidak lagi hanya digunakan sebagai pengganti mesin tik ataupun alat hitung, namun kini juga banyak digunakan dalam membantu pembuatan keputusan penting. Untuk itu, informasi yang disimpan memerlukan pengamanan yang dapat melindungi terhadap akses orang yang tidak berhak.

Orang-orang yang menginginkan informasi yang dimilikinya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara untuk mengamankannya. Salah satu cara yang dapat dilakukan untuk melindungi informasi tersebut adalah dengan mengacak data atau dengan menyandikan atau mengkodekan data (informasi) ke dalam suatu bentuk untuk menyembunyikan substansinya. Kegiatan pengamanan data ini disebut dengan kriptografi. Kriptografi merupakan ilmu pengetahuan bidang matematika, karena landasan yang digunakan pada sebagian besar konsep di dalam kriptografi adalah matematika [8].

Kriptografi memiliki berbagai langkah-langkah dalam menyandikan informasi, langkah-langkah tersebut disebut juga algoritma kriptografi [7]. Beberapa algoritma kriptografi telah dipublikasikan seperti *DES (Data Encryption Standard), AES (Advanced Encryption Standard), Elgamal, Knapsack, Neokoen, Eliptic Curve Cryptosystem, RSA (Rivest Shamir Adleman)* dan lain sebagainya [6]. Berkaitan dengan hal di atas, algoritma kriptografi *Noekoen* telah diaplikasikan oleh Jaya [5]. Sedangkan dalam tugas akhir ini akan diaplikasikan algoritma kriptografi RSA, yang akan dicksekusi dengan menggunakan bahasa program Borland Delphi 6.0.

1.2. Permasalahan

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan informasi atau data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* tersebut dapat ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali. Salah satu proses pentransformasian dapat dilakukan dengan algoritma RSA. RSA adalah singkatan dari nama-nama penemunya yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman [8].

Tugas akhir ini akan membahas mengenai algoritma RSA tersebut, dengan inti permasalahannya adalah "Bagaimana mengaplikasikan Algoritma RSA dalam sebuah program enkripsi atau dekripsi ?"

Dengan menggunakan program yang dikembangkan dalam tugas akhir ini, pemakai dapat mengamankan datanya sehingga tidak dapat diakses oleh orang yang tidak berhak, pemakai tidak perlu mempelajari tata cara pemakaian program yang rumit, karena hanya terdapat beberapa perintah yang mudah diingat.

BAB V

PENUTUP

5.1. Kesimpulan

Beberapa buah kesimpulan yang dapat diambil setelah melaksanakan Tugas Akhir ini adalah :

1. Pada tugas akhir ini penulis berhasil membuat program simulasi algoritma kriptografi RSA dengan bahasa pemograman Borland Delphi 6.0 dan berjalan dengan baik sehingga dapat menerangkan cara kerjanya
2. Algoritma RSA berisi pemfaktoran yang amat rumit sehingga tidak mudah dibobol. Semakin besar ukuran kunci yang digunakan semakin tinggi pula tingkat keamanan informasi yang dienkripsi.
3. Dua buah bilangan bulat nonnegatif a dan b serta x dan y dalam persamaan $ax + by = d$, diperoleh nilai d yaitu pembagi bilangan terbesar dari a dan b atau PBB(a, b) dan d adalah bilangan bulat.
4. Ciphertext yang dihasilkan program tergantung pada *plaintext* dan ukuran kunci yang digunakan.
5. Ciphertext yang dihasilkan dari pengenkripsi teks memiliki ukuran lebih besar daripada *plaintext*, karena adanya penambahan informasi pada *ciphertext*, sedangkan *chipertext* yang dihasilkan dari pengenkripsi file memiliki ukuran sama besar dengan *plaintext*.

DAFTAR PUSTAKA

[1] Davis, Tom.2003. *RSA Encryption.* Geometer

[2] Durbin, John. R. 2000. *Modern Algebra An Introduction.* New York. John Wiley and Sons, Inc.

[3] Hidayat, Taufik. *Sistem Kriptografi IDEA.* ITB Press. Bandung.

[4] Iqbal, Muhammad. 2006. *Studi Teknis Metode Enkripsi Rsa Dalam Perhitungannya.* ITB Press. Bandung.

[5] Jaya N, I Made Ari, 2003. *Penyandian Data Dengan Algoritma Kriptografi Nekoen. Tesis-Pasca Sarjana,* tidak diterbitkan.

[6] Menezes, A., Van Oorschot dan S. Vanstone. 1997. *Handbook Of Applied Cryptography.* ISC Press.

[7] Munir, Rinaldi. 2005. *Matematika Diskrit,* edisi ke-3. Informatika. Bandung.

[8] Munir, Rinaldi. 2006. *Kriptografi.* Informatika. Bandung.

[9] Mulayana, Satria Budi. 2002. *Implementasi Algoritma Enkripsi Rijndael (Gladman) Dalam OpenSSI-0.9.7. Skripsi-S1,* Tidak diterbitkan.

[10] Pranata, Anthony. 2003. *Pemograman Borland Delphi 6.0.* Andi Press. Yogyakarta.