ENKRIPSI DAN DEKRIPSI DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI BLUM-GOLDWASSER

SKRIPSI SARJANA MATEMATIKA

Oleh

Sherly Al Varika
05 134 030

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS ANDALAS
PADANG
2009

ABSTRAK

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi (*encrypt*) maupun dekripsi (*decrypt*) data. Enkripsi adalah suatu proses untuk mengubah plainteks menjadi cipherteks dan dekripsi adalah proses untuk mengembalikan cipherteks menjadi plainteks. Berdasarkan jenis kunci yang digunakan, algoritma kriptografi dikelompokan menjadi dua bagian, yaitu algoritma simetris dan algoritma asimetris.

Algoritma Blum-Goldwasser yang ditemukan oleh Manuel Blum dan Shafi Goldwasser pada tahun 1984 ini merupakan algoritma kriptografi asimetris yang menggunakan dua kunci yaitu kunci publik dan kunci privat. Tingkat keamanan algoritma ini didasarkan pada masalah faktorisasi bilangan bulat, yaitu sulitnya memfaktorkan bilangan bulat n yang merupakan komposit dari bilangan-bilangan prima yang cukup besar, misal p dan q. Algoritma Blum-Goldwasser mempunyai kunci publik berupa satu bilangan dan kunci privat berupa empat bilangan. Algoritma ini melakukan proses enkripsi pada blok-blok plainteks dan proses dekripsi pada blok-blok cipherteks.

Pembahasan algoritma *Blum-Goldwasser* meliputi konsep matematis yang melandasinya dan proses penyandiannya. Algoritma Blum-Goldwasser ini diimplementasikan ke dalam bahasa program MS-Visual Basic 6.0 agar aplikasi ini dapat digunakan untuk menyandikan pesan (teks).

Kata Kunci : *kriptografi, enkripsi, dekripsi, Blum-Goldwasser, MS-Visual Basic 6.0*

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dewasa ini kemajuan teknologi di bidang komputer memungkinkan ribuan orang dan komputer di seluruh dunia terhubung dalam satu dunia maya yang dikenal sebagai internet. Demikian juga dengan ratusan organisasi, diantaranya lembaga negara, lembaga keuangan, militer, perusahaan, dan institusi pendidikan. Penggunaan komputer tidak hanya sebagai alat hitung ataupun pengganti mesin tik saja tapi juga sebagai alat untuk menyimpan informasi-informasi penting. Tapi sayangnya, kemajuan teknologi juga selalu diikuti dengan sisi buruknya.

Salah satu dari sisi buruk tersebut adalah rawannya keamanan data sehingga menimbulkan tantangan dan tuntutan akan tersedianya suatu sistem pengamanan data yang sama canggihnya dengan kemajuan teknologi komputer itu sendiri. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan dari informasi rahasia ini. Salah satu cara yang digunakan adalah mengubah data ke dalam kode-kode tertentu sehingga informasi yang disimpan atau ditransmisikan melalui jaringan yang tidak aman, misalnya internet, tidak dapat dibaca oleh siapapun kecuali orang-orang yang berhak.

Teknik pengamanan data ini dikenal dengan kriptografi. Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi (*encrypt*) maupun dekripsi (*decrypt*) data [9].

Kriptografi modern menyelesaikan masalah enkripsi dan dekripsi dengan merahasiakan kunci tanpa harus merahasiakan algoritmanya. Karena keamanan

bergantung pada kerahasian kunci, maka algoritma yang dibentuk dapat dianalisis dan dipublikasikan sehingga memungkinkan pengembangan yang lebih baik [9].

Beberapa algoritma kriptografi telah dipublikasikan, diantaranya *DES* (*Data Encryption Standard*), *AES* (*Advanced Encryption Standard*), *RSA* (*Rivest Shamir Adleman*), *ECC*(*Eliptic Curve Cryptosystem*), *ElGamal*, *Knapsack*, *Rabin*, dan *Blum-Goldwasser* [4].

Algoritma kriptografi Blum-Goldwasser merupakan algoritma kunci publik yang ditemukan oleh Manuel Blum dan Shafi Goldwasser pada tahun 1984. Sampai saat sekarang algoritma ini masih dipercaya sebagai salah satu metode penyandian karena tingkat keamanan algoritma ini didasarkan pada masalah faktorisasi bilangan bulat, yaitu sulitnya memfaktorkan bilangan bulat n yang merupakan komposit dari bilangan-bilangan prima yang cukup besar, misal p dan q. Keamanan algoritma ini juga terletak pada sulitnya memprediksi barisan bit acak yang diperoleh dari hasil akhir algoritma Blum-Blum Shub yang bergantung pada kunci publik n.

Dalam tugas akhir ini, akan dijelaskan cara kerja algoritma kriptografi *Blum-Goldwasser* dan diimplementasikan menjadi sebuah aplikasi yang dieksekusi dengan menggunakan bahasa program MS-Visual Basic 6.0.

1.2 Perumusan Masalah

Sesuai dengan salah satu tujuan dasar penyandian, yaitu menjaga kerahasiaan data, kriptografi mentransformasikan data jelas ke dalam bentuk data sandi yang tidak dapat dikenali. Cipherteks inilah yang kemudian dikirimkan oleh pengirim kepada penerima. Setelah sampai di penerima, cipherteks tersebut ditransformasikan kembali ke dalam bentuk plainteks agar dapat dikenali. Salah

BAB V

PENUTUP

5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil setelah melaksanakan tugas akhir ini adalah :

1. Algoritma Blum-Goldwasser menggunakan beberapa algoritma dalam proses penyandianya, yaitu algortima Euclide, algoritma Euclide yang diperluas, algoritma Blum Blum Shub dan algoritma eksponentasi dengan pengakaran dan perkalian berulang.
2. Cipherteks yang dihasilkan bergantung pada plainteks dan ukuran kunci yang digunakan.
3. Cipherteks yang dihasilkan dari proses enkripsi memiliki ukuran yang lebih besar daripada plainteks.
4. Keamanan algoritma kriptografi Blum-Goldwasser terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

5.2 Saran

Adapun beberapa saran yang dapat digunakan untuk pengembangan lebih lanjut tugas akhir ini adalah sebagai berikut :

1. Melakukan perbaikan pada manajemen kunci publik dan kunci privat, termasuk peningkatan keamanan pada keduanya.

DAFTAR PUSTAKA

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

[2] Elviyenti, M. 2007. *Penyandian Data dengan Algoritma Kriptografi RSA*. Skripsi-S1, Tidak diterbitkan

[3] Alam, M. A. J. 2002. *Belajar Sendiri Microsoft Visual Basic versi 6.0*. Gramedia. Jakarta

[4] Menezes, A., Van Oorschot and S. Vanstone. 1997. *Handbook of Applied Cryptography*. CRC Press

[5] Munir, R. 2005. *Matematika Diskrit*, edisi ke-3. Informatika. Bandung

[6] Munir, R. 2006. *Kriptografi*. Informatika. Bandung

[7] Schneier, B. 1996. *Applied Cryptography 2nd*. John Wiley & Sons, Inc. New York

[8] Siang. J. J. 2004. *Matematika Diskrit dan Aplikasinya pada Ilmu Komputer*. Andi Press. Yogyakarta

[9] Simarmata. J. 2006. *Pengamanan Sistem Komputer*. Andi Press. Yogyakarta