IMPLEMENTASI TEKNIK KRIPTOGRAFI MENGGUNAKAN METODA RSA UNTUK PENGAMANAN DATABASE

TUGAS AKHIR

Diajukan untuk salah satu syarat
Mendapatkan Gelar Ahli Madya

Oleh:

NOVITRI WULANDARI
05 085 021

Program Studi Teknik Telekomunikasi Multimedia
Jurusan Teknik Elektro

DEPARTEMEN PENDIDIKAN NASIONAL
UNIVERSITAS ANDALAS
UPT PERPUSTAKAAN

POLITEKNIK UNIVERSITAS ANDALAS
2008

ABSTRAK

Saat ini, banyak cara yang digunakan untuk melindungi data yang disimpan ataupun dikirim melalui media elektronik. Salah satunya adalah RSA(*Rivest-Shamir Adleman*). RSA adalah sistem sandi yang saat ini menjadi standart de facto dunia. RSA merupakan metode penyandian yang sangat kokoh untuk mengatasi masalah keamanan data pada suatu jaringan komputer. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Tulisan ini membahas tentang pengamanan database menggunakan teknik kriptografi. Program ini dirancang dengan komputer memakai perangkat lunak Visual Basic 6.0.

Kata kunci : RSA (*Rivest-Shamir Adleman*).

BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Berbagai organisasi, perusahaan, atau pun pihak – pihak lain telah memanfaatkan teknologi basis data untuk menyimpan dan mengelola data organisasi atau perusahaannya. Saat ini, keamanan terhadap data yang tersimpan dalam basis data sudah menjadi persyaratan mutlak. Pengamanan terhadap jaringan komputer yang terhubung dengan basis data sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak – pihak yang langsung berhubungan dengan basis data seperti administrator basis data. Hal ini menyebabkan pengguna basis data harus menemukan cara untuk mengamankan data tanpa campur tangan administrator basis data. Kriptografi dapat digunakan untuk mengamankan data. Oleh karena itu, pengguna basis data membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. Penerapan kriptografi pada Tugas Akhir ini akan difokuskan bagaimana kriptografi dapat mengamankan data dan tetap memperhatikan integritas data dan kewenangan setiap pengguna basis data. Algoritma kriptografi yang akan digunakan ialah algoritma RSA yang mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci rahasia hanya pihak-pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi.

1.2. TUJUAN

Tujuan dari pembuatan tugas akhir ini adalah:

1. Membuat sistem yang dapat melindungi database menggunakan algoritma RSA.

2. Menganalisa cara kerja dari algoritma RSA dibanding dengan metoda password.

1.3. PERUMUSAN MASALAH

Dari penjelasan diatas dapat disimpulkan bahwa perlunya kerahasiaan sebuah data agar data tersebut tidak dapat dirusak oleh pihak-pihak yang tidak bertanggung jawab, untuk itu diperlukan sebuah sistem yang dapat melindungi kerahasiaan data tersebut. Salah satu cara yang dapat dilakukan adalah menggunakan Kriptografi.

1.4.BATASAN MASALAH

Agar pengerjaan Tugas Akhir ini tidak keluar dari tujuan yang diinginkan,maka masalah dalam pembuatan Tugas Akhir ini akan dibatasi pada :

1. Melindungi database hanya menggunakan algoritma RSA

2. Data yang diamankan adalah data gaji dalam database

3. Untuk akses data hanya menggunakan kode password

1.5. METODOLOGI PENYELESAIAN TUGAS AKHIR

Metoda penulisan yang digunakan dalam pembuatan Tugas Akhir adalah :

a. Studi Literatur

Pada tahap ini dipelajari bahan-bahan literatur yang berhubungan dengan topik serta beberapa sumber yang berkaitan dengan kriptografi dan beberapa pendekatan lain

BAB V

PENUTUP

5.1 Kesimpulan

Dari program diatas dapat disimpulkan bahwa :

1. Untuk menembus keamanan RSA, pihak penyerang memfaktorkan nilai n menjadi p dan q yang sesuai dengan kunci publik. Untuk memperkuat tingkat keamanan, sebaiknya digunakan bilangan prima p dan q yang besar, sehingga pihak penyerang akan kesulitan dan membutuhkan waktu yang sangat lama untuk memfaktorkan n.
2. Dalam proses pembuatan kunci publik dan kunci privat, terdapat beberapa faktor yang menjadi pertimbangan, yaitu ukuran dari kunci, penentuan nilai p dan q agar sulit untuk dibobol, dan kemungkinan kelemahan yang dapat diketahui saat data selesai dienkripsi

5.2 Saran

Agar pembuatan program ini lebih baik maka disarankan :

1. Menggunakan algoritma yang terbaru daripada algoritma RSA, agar program ini dapat berfungsi lebih baik, dan kelengkapan sistem yang lebih memadai.
2. Menggunakan kunci publik yang lebih panjang, dimana semakin panjang kunci publik yang digunakan, maka usaha yang harus dikeluarkan untuk memecahkan kunci tersebut akan lebih lama. Pada saat ini dianjurkan untuk menggunakan sistem RSA dengan kunci publik 1024 bit.

DAFTAR PUSTAKA

Raharjo Budi, 1998. *Keamanan Sistem Informasi Berbasis Internet*, PT. Insan Indonesia–Bandung & PT. INDOCISC-Jakarta

Http : // www.blogger.com/css/blog.controls.css

Davis, Tom. 2003. *RSA Encryption* http://www.geometer.org/mathcir cles/RSA.pdf

Http : //id.wikipedia.org/wiki/RSA

Tedi Heriyanto, 2000. *Pengenalan Algoritma RSA*

Http : //www.AsciiTable.com

RSA Security - 3_1 RSA. (2008). http://www.rsasecurity.com/rsalabs/node.asp?id =2213.

RSA - Wikipedia Indonesia, ensiklopedia bebas berbahasa Indonesia. (2008). http://id.wikipedia.org/wiki/RSA.