TUGAS AKHIR

IMPLEMENTASI KEAMANAN DATA DENGAN METODE PGP (PRETTY GOOD PRIVACY) BERBASIS JAVA DAN MY SQL

Diajukan sebagai salah satu syarat
untuk memperoleh gelar Ahli Madya

Oleh :

NURHAYATI
06 085 009

DIREKTORAT PENDIDIKAN PROFESIONAL
UNIVERSITAS ANDALAS
UPT PERPUSTAKAAN

JURUSAN ELEKTRO
PROGRAM STUDI TEKNIK TELEKOMUNIKASI
POLITEKNIK UNIVERSITAS ANDALAS
PADANG
2010

ABSTRAK

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari sistem informasi. Dalam hal ini, sangat terkait dengan betapa pentingnya informasi dan data tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi akan tidak berguna lagi apabila di tengah jalan informasi itu disadap(dihecker) oleh orang yang tidak bertanggungjawab atau berhak. Untuk mengatasi hal tersebut diperlukan adanya sistem pengamanan terhadap data yang dikenal sebgai ilmu kriptografi. Berbagai jenis metode kriptografi juga dikembangkan untuk membuat pengamanan data semakin baik dan tidak mudah dilihat oleh pihak lain. Salah satu metode enkripsi yang sangat popular saat ini adalah pengamanan data dengan metode PGP (Pretty Good Privacy) yang menggunakan algoritma asimetrik dengan dua kunci yang berbeda, disebut juga pasangan kunci (key pair) untuk proses enkripsi dan dekripsi.

Program ini memungkinkan seorang pengirim pesan mengirimkan pesanya kepada pihak lain dengan data yang telah terenkripsi menggunakan kunci publik si penerima. Pada sisi penerima pembacaan pesan yang diterima dalam bentuk enkripsi harus didekripsikan terlebih dahulu dengan kunci pribadi milik sipenerima.

program ini dirancang dengan menggunakan bahasa pemograman Java NetBeans6.5 dan didukung dengan pemograman My SQL sebagai database dari program. Untuk melakukan pengiriman pesan dalam bentuk terenkripsi kita harus memiliki kunci publik dari sipenerima pesan sedangkan kunci pribadi milik kita digunakan untuk proses enkripsinya. Pada sisi penerima pesan hanya dapat didekripsi menggunakan kunci pribadi milik si penerima.

Kata Kunci : Kriptografi, Java, PGP, My SQL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan dan perkembangan teknologi informasi dewasa ini telah berpengaruh pada hampir semua aspek kehidupan manusia, tak terkecuali dalam hal berkomunikasi. Dengan adanya internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan murah. Namun di sisi lain, ternyata internet tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap penyadapan informasi oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Oleh karena penggunaan internet yang sangat luas seperti pada bisnis, perdagangan, bank, industri dan pemerintahan yang umumnya mengandung informasi yang bersifat rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia ini.

Keamanan ini dapat dipecahkan dengan metode kriptografi yang tepat. Para ahli kriptografi pun mengembangkan sebuah teknologi yang mereka sebut dengan *Pretty Good Privacy (PGP)* yang bisa digunakan untuk menjamin keamanan sebuah *email,* sehingga masalah - masalah di atas dapat dipecahkan dengan baik dan dengan biaya yang murah.

Penggunaan PGP sebagai media untuk melakukan kriptografi ini sangat baik sekali karena PGP menggunakan sistem kunci asimetris dalam melakukan proses deskripsi/enkripsi yang mana kunci pada saat melakukan proses enkripsi berbeda

dengan kunci pada proses deskripsi sehinngga keamanan benar-benar terjaga. Seseorang bisa saja mengetahui apa kunci yang digunakan saat melekukan enkripsi tapi orang tersebut tidak akan bisa membuaka atau membaca kembali pesan tersebut bila tidak mengetahui kunci yang digunakan untuk proses deskripsi

1.2 Tujuan

Tujuan dari tugas akhir ini adalah untuk mengimplementasikan teknik enkripsi data dengan metode PGP pada aplikasi java dalam mengamankan sebuah data.

1.3 Perumusan Masalah

Adapun permasalahan yang dibahas dalam pembuatan tugas akhir ini adalah :

1. Penanganan Masalah Otomatisasi Kriptografi Kunci Enkripsi
2. Implementasai PGP dalam mengamankan sebuah data

1.4 Batasan Masalah

Pembuatan tugas akhir ini memfokuskan pada pengamanan data dengan menggunakan menggunakan metode PGP dalam aplikasi java. Pengamanan yang dilakukan yaitu membuat pesan dalam bentuk asli menjadi pesan acak atau dienkripsi.

1.5 Metoda Penulisan

Metoda penulisan yang dipakai dalam pembuatan tugas akhir ini adalah :

BAB V

PENUTUP

5.1 Kesimpulan

Setelah dilakukan pengujian dan analisa dari pengamanan data dengan metode PGP pada aplikasi java, maka dapat ditarik kesimpulan sebagai berikut :

1. Pengamanan pesan ini dirancang untuk mengamankan pesan yang dikirim agar tidak terjadi penyadapan terhadap pesan sehingga pesan yang dikirim benar-benar terjaga keasliannya dengan mengguanakan bahasa pemograman Java sebagai media untuk melakukan pengamanan.
2. Semaikin banyak kombinasi karakter yang dgunakan dalam penciptaan kunci maka semakin sulit bagi pihak lain untuk mengetahui identitas kunci kita sehinngga keamanan pesan semakin terjaga.
3. PGP menggunakan sistem asimetrik key yang mana kunci saat mengenkripsi dan deskripsi tidak sama dalam mengamankan data. Pada saat mengirim pesan kita menggunakan kunci private pengirim untuk menenkripsi pesan dan kunci publik penerima untuk mengirimkan pesannya. Pada sisi penerima digunakan kunci private milik penerima untuk melakukan proses deskripsi data.

5.2 Saran

Dalam pembuatan Tugas Akhir ini, penulis ingin menyampaikan beberapa saran agar Tugas Akhir ini dapat dikembangkan lebih baik, diantaranya sebagai berikut :

DAFTAR PUSTAKA

Ariyus, Dony, 2008. *"Pengantar Ilmu Kriptografi"*. Ditemukan tanggal 23 Desember 2009. Dari http://Ilmu Komputer.com jam 19:15

Baldwin, *"Kriptografi Menggunakan Kunci Publik Menggunakan Java 101"* Ditemukan Tanggal 23 Januari 2010. Dari http://www.developer.com jam 20:05

file:///E:/bahan%20PGP/PGP1/book3.htm#v=onepage&q=&f=false Ditemukan tanggal 13 November 2009 jam 11:45

http://www.scribd.com/doc/14432602/PGP Ditemukan Tanggal 12 Oktober 2009 jam 16:10

Stalings, William, 2000. *Pengamanan Jaringan Komputer*. Ditemukan Tanggal 7 Oktober 2009. Dari http://ilmu Komputer.com jam 14:31

Tim Pengembangan Jeni, 2007. Pengenalan Pemograman Java1