Jurnal Mahajana Inforamasi, Vol.1 No 1, 2016
e-ISSN: 2527-8290

KEAMANAN BASIS DATA DENGAN TEKNIK ENKRIPSI

Harold Situmorang
Program Sutdi Sistem Informasi Universitas Sari Mutiara Indonesia
haroldsitumorang@yahoo.co.id

Abstrak

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 dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, otentikasi, dan ketiadaan penyangkalan. Oleh karena itu, pengguna basis data membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya.

Kata kunci : *Kriptografi*, *Basis Data*

1. Pendahuluan

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 tuisan ini akan difokuskan bagaimana kriptografi dapat mengamankan data sampai pada level baris (*row*) dan kolom (*field*) dengan tetap memperhatikan integritas data dan kewenangan setiap pengguna basis data. Algoritma kriptografi yang akan digunakan ialah algoritma kriptografi simetris dan bersifat *stream cipher* sehingga data hasil enkripsi (cipherteks) mempunyai ukuran yang sama dengan data asli (plainteks). Teknik kriptografi simetris dipilih karena diharapkan dengan algoritma ini proses enkripsi – dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan dengan algoritma kriptografi kunci publik (asimetris).

1. Tinjauan Pustaka

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. Untuk melaksanakan tujuan tersebutlah dirancang suatu sistem keamanan yang berfungsi melindungi sistem informasi. Salah satu upaya pengamanan

sistem informasi yang dapat dilakukan adalah kriptografi. 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.

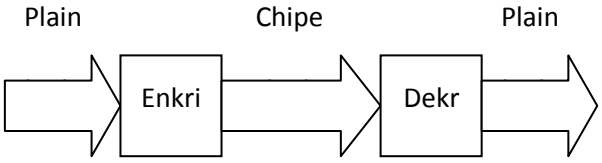
2.1 Mekanisme Kriptografi

Suatu sistem kriptografi (kriptosistem) bekerja dengan cara menyandikan suatu pesan menjadi suatu kode rahasia yang dimengerti oleh pelaku sistem informasi saja. Pada dasarnya mekanisme kerja semacam ini telah dikenal sejak jaman dahulu. Bangsa Mesir kuno sekitar 4000 tahun yang lalu bahkan telah mempraktekkannya dengan cara yang sangat primitif.

Dalam era teknologi informasi sekarang ini, mekanisme yang sama masih digunakan tetapi tentunya implementasi sistemnya berbeda. Sebelum membahas lebih jauh mekanisme kriptografi modern, berikut ini diberikan beberapa istilah yang umum digunakan dalam pembahasan kriptografi.

1. *Plaintext*
   Plaintext (message) merupakan pesan asli yang ingin dikirimkan dan dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.
2. *Chipertext*
   Chipertext merupakan pesan yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.
3. *Chiper*
   Chiper merupakan algoritma matematis yang digunakan untuk proses penyandian plaintext menjadi ciphertext.
4. *Enkripsi*
   Enkripsi (*encryption*) merupakan proses yang dilakukan untuk menyandikan plaintext sehingga menjadi chipertext.
5. *Dekripsi*
   Dekripsi (*decryption*) merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari chipertext.
6. *Kriptosistem*

Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi. Urutan-urutan proses kriptografi dapat digambarkan sebagai berikut.



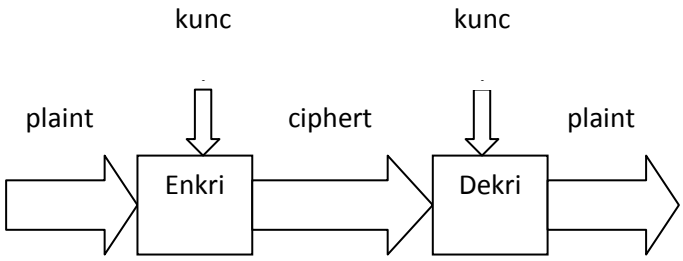
Gambar 1. Mekanisme kriptografi

Prosesnya pada dasarnya sangat sederhana. Sebuah plaintext (m) akan dilewatkan pada proses enkripsi (E) sehingga menghasilkan suatu ciphertext (c). Kemudian untuk memperoleh kembali plaintext, maka ciphertext (c) melalui proses dekripsi (D) yang akan menghasilkan kembali plaintext (m). Secara matematis proses ini dapat dinyatakan sebagai,

$$E(m) = c$$
$$D(c) = m$$
$$D(E(m)) = m$$

Kriptografi sederhana seperti ini menggunakan algoritma penyandian yang disebut *cipher*. Keamanannya bergantung pada kerahasiaan algoritma penyandian tersebut, karena itu algoritmanya harus dirahasiakan. Pada kelompok dengan jumlah besar dan anggota yang senantiasa berubah, penggunaannya akan menimbulkan masalah. Setiap ada anggota yang meninggalkan kelompok, algoritma harus diganti karena anggota ini dapat saja membocorkan algoritma.
Kriptografi modern selain memanfaatkan algoritma juga menggunakan kunci (*key*) untuk memecahkan masalah tersebut. Proses enkripsi dan dekripsi dilakukan dengan menggunakan

kunci ini. Setiap anggota memiliki kuncinya masing-masing yang digunakan untuk proses enkripsi dan dekripsi yang akan dilakukannya. Dengan demikian ada sedikit perubahan yang harus dilakukan pada mekanisme yang digambarkan pada gambar 1 menjadi seperti gambar 2 berikut ini.



Gambar 2. Kriptografi berbasis kunci

Mekanisme kriptografi seperti ini dinamakan kriptografi berbasis kunci. Dengan demikian kriptosistemnya akan terdiri atas algoritma dan kunci, beserta segala plaintext dan ciphertextnya.

Persamaan matematisnya menjadi seperti berikut,

$$E_e(m) = c$$
$$D_d(c) = m$$
$$D_d(E_e(m)) = m$$

dengan,

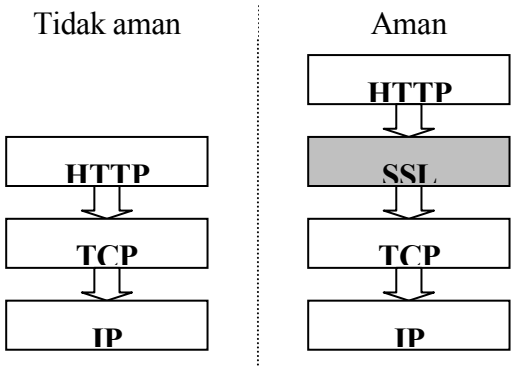
e = kunci enkripsi

d = kunci dekripsi

2.2 Penggunaan Sistem Kriptografi

Sistem kriptografi pada era sistem informasi ini telah dimanfaatkan dalam pengamanan suatu sistem informasi. Pada jaringan TCP/IP (*Transfer Control Protocol/Internet Protocol*) misalnya, kriptografi telah dimanfaatkan pada protokol S/HTTP. Protokol S/HTTP (*Secure Hypertext Transfer Protocol*) saat ini digunakan untuk transaksi HTTP dengan memanfaatkan kriptografi sebagai mekanisme untuk menyandikan pesan yang dikirim.

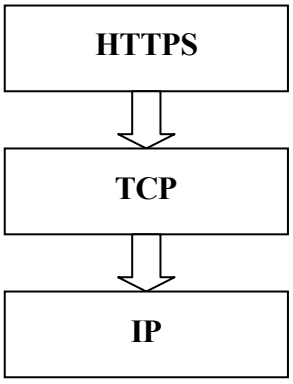
Gambar dibawah ini menunjukkan mekanisme enkapsulasi data pada jaringan TCP/IP tanpa dan dengan kriptografi



Gambar 3. Kriptografi pada TCP/IP

Dapat dilihat bahwa ada penambahan satu layer baru yang dinamakan sebagai SSL (*Secure Socket Layer*). Layer ini berfungsi untuk melaksanakan mekanisme kriptografi terhadap informasi sebelum dilakukan enkapsulasi dan pengiriman data. Penambahan layer SSL ini menyebabkan terbentuknya protokol baru yang dinamakan HTTPS, menggantikan protokol HTTP untuk transaksi HTTP yang aman. Protokol ini digunakan untuk mengamankan transaksi-transaksi data pada web-web *e-commerce.*

Gambar berikut menunjukkan protokol HTTPS tersebut.



Gambar 4. Protokol HTTPS

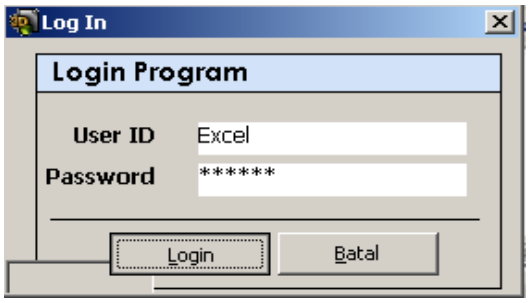
2. ANALISIS

Analisa sistem yang sedang berjalan pada sebuah program distribusi kartu pada sebuah perusahaan telekomunikasi di Medan menunjukkan bahwasanya dalam akses keamanan dalam program distribusi kartu tersebut sangat tidak terjamin dan semua pegawai ataupun orang lain dapat menggunakan program tersebut sehingga yang nantinya akan mengakibatkan kesalahan data dan kerusakan dalam program kerja dimana laporan-laporan yang akan dihasilkan tidak sesuai dengan fakta yang terjadi di lapangan. Misalnya jika ada pegawai atau orang luar yang dapat menggunakan program tersebut maka dia dapat melakukan transaksi permintaan kartu yang fiktif dari sebuah toko distributor maka data transaksi tersebut akan masuk kedalam laporan dan pihak perusahaan akan membuat laporan tersebut ataupun laporan permintaan tersebut langsung akan direalisasikan dan perusahaan akan mengirim barang permintaan toko distributor dan ketika diantar bahwasanya toko tidak pernah memesan barang tersebut.

3. IMPLEMENTASI

Pada tahap implementasi ini penulis mencoba melakukan percobaan pengamanan database login pada sebuah program distribusi barang dengan menggunakan enkripsi pada data password pengguna sehingga pengguna yang berhak saja yang dapat menggunakan program sistem informasi kartu tersebut.

Untuk dapat masuk ke dalam menu program sistem informasi kartu setiap pengguna harus melakukan login program dengan memasukkan User ID dan Password bila User ID dan Password sudah terdaftar dan sesuai dengan yang ada didatabase maka program sistem informasi kartu dapat terbuka (digunakan). Jika User ID dan Password tidak terdaftar dan salah maka program sistem informasi kartu tidak dapat digunakan (terbuka). Terlihat pada gambar berikut menu login untuk masuk ke dalam program sistem informasi kartu.



Gambar 5. Menu login

Untuk melakukan login pengguna harus memasukkan User ID selanjutnya memasukkan passwordnya kemudian tekan login. Dan bila pengisian User ID dan Password anda ada yang salah dapat menekan tombol batal. Setelah tombol login ditekan dan User ID dan password sesuai dengan didatabase maka pengguna dapat melihat menu utama program sistem informasi kartu seperti pada gambar 6 berikut.

Gambar 6. Menu utama program

Bagi pengguna yang ingin mendaftar atau mengubah password lamanya dapat menggunakan user manangement kemudian pilih user account.

Gambar 7. Menu Uase Account

Setelah masuk kedalam menu user account. Bagi pengguna yang mendaftar dapat mengklik tombol new kemudian isikan User ID dan Password dan isi ulang Password dan pilih statusnya. Pada gambar 7 ditampilkan contoh pengisian user account yang baru.

Gambar 8. Tampilan pengisian user account

Setelah seluruh inputan diisi maka dilanjutkan untuk menyimpan atau bila anda ada merasa ragu dengan User ID ataupun pengisian password dan ulangi password ataupun salah dalam memilih status dapat menekan tombol cancel. Dan untuk keluar dari program user account dapat mengklik tombol close.

Gambar 9. Bentuk pengisian user account

Setelah data-data yang harus diisi telah penulis isi dan penulis telah menyimpannya maka data penulis tampak pada tabel user id didalam user account dimana ditampilkan pada tabel tersebut seluruh pengguna yang telah terdaftar dengan statusnya.

Selanjutnya kita dapat melihat bentuk basisdata pengenkripsian dari pengisian data-data pada menu user account pada tabel database login seperti yang ditunjukkan pada gambar 10 berikut.

Gambar 10. Tabel database login

Pada gambar diatas terlihat bentuk pengenkripsian daripada database dimana yang dienkripsi adalah data password dari user id. Dengan pengenkripsian tersebut seseorang yang ingin menggunakan program sistem informasi kartu tidak dapat menggunakan user id yang lain untuk masuk ke dalam program sistem informasi kartu karena data passwordnya telah terenkripsi.

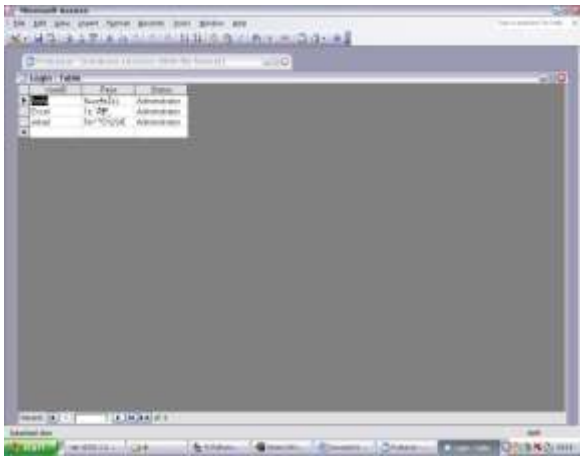
Gambar 11. Penggantian password lama

Disini penulis mencoba untuk mengganti password lamanya dengan password baru. Dalam pergantian password ini pengguna harus mengisi data-data User ID dan password lama serta statusnya. Setelah data-data tersebut diisi maka tekan tombol lanjut.

Setelah tombol lanjut ditekan maka akan muncul pengisian data-data untuk pengisian data-data baru anda seperti halnya pada gambar 11 Setelah

data-data baru penulis isi kemudian penulis menyimpannya.

Berikut penulis tampilkan database dari data-data penulis yang baru seperti pada gambar 12 berikut.



Gambar 12. Bentuk database login

4. Kesimpulan

Setelah penulis menguraikan semuanya tentang perancangan dan implementasi dari enkripsi data login ini, maka penulis mengambil beberapa kesimpulan yaitu :

1. Dengan pengenkripsian database pada sebuah program dapat membantu pengamana program dari pengguna yang tidak bertanggung jawab.
2. Banyaknya bentuk-bentuk algoritma untuk metode enkripsi dan deskripsi sebagai pengembangan ilmu pengetahuan tentang kriptografi sekuriti sistem.
3. Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah dengan kriptografi sekuriti sistem.

DAFTAR PUSTAKA

A. Rahmani, *Implementasi Teknik Kriptografi Blowfish untuk Pengamanan Basis Data*, Tesis Magister Departemen Teknik Informatika, ITB, 2003.

A. Silberschatz, H. F. Korth. Dan S. Sudarshan, *Database System Concepts, 4th Edition*, McGraw – Hill, 2002.

B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition*,John Wiley & Sons, Inc, 1996.

B. Sukmawan, *RC4 Stream Cipher*, 1998.

B. Trower, *Crypt Data Packaging*, Trantor Standard Systems Inc.

Ir. Fathansyah, *Basis Data*, Informatika, Bandung, 1999.

R. Munir, *Bahan Kuliah IF5054 Kriptografi*, Departemen Teknik Informatika, ITB, 2004.

T. Marcus, A. Prijono dan J.Widiadhi, *DELPHI DEVELOPER dan SQL Server 2000*, Informatika, Bandung, 2004.