ANALISIS DAN IMPLEMENTASI ENKRIPSI BASIS DATA DENGAN ALGORTIMA KRIPTOGRAFI BLOWFISH

Naskah Publikasi

disusun oleh

Ari Suhendra

06.11.1120

kepada
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2012

NASKAH PUBLIKASI

ANALISIS DAN IMPLEMENTASI ENKRIPSI BASIS DATA DENGAN ALGORTIMA KRIPTOGRAFI BLOWFISH

disusun oleh

Ari Suhendra
06.11.1120

Dosen Pembimbing,

Dr. Ema Utami, S.Si, M.Kom
NIK. 190302037

Tanggal, 15 juni 2012

Ketua Jurusan
Teknik Informatika

Sudarmawan, MT
NIK. 190302035

ANALYSIS AND IMPLEMENTATION DATABASE ENCRYPTION WITH CRYPTOGRAPHY ALGORITHM BLOWFISH

ANALISIS DAN IMPLEMENTASI ENKRIPSI BASIS DATA DENGAN ALGORITMA KRIPTOGRAFI BLOWFISH

Ari Suhendra
Ema Utami
Jurusan Teknik Informatika
STMIK AMIKOM YOGYAKARTA

ABSTRACT

Along with the development of technology in the business world, the database system has become a symbol of one of the most valuable forms of assets. The database has become a requirement in some organizations and commercial companies at the moment such as business, banking, education, employment, and others. With the increasingly wide use of database systems, the protection of the information stored within it becomes very necessary to protect against a variety of threats such as reading data, data manipulation and destruction of data by unauthorized parties.

Cryptographic techniques by using the blowfish algorithm implemented in a programming language can overcome the abuse of the right of access to the database by unauthorized parties. The process of encoding the cryptography consists of two phases, namely encryption and decryption.

From the test results, it can be done in the implementation of the Windows operating system work. All types of files that have been tested such as Microsoft SQL server files (.mdf), Images (.jpg, .gif, .bmp, .png, etc), Video (.wmp, .mpeg, .mp4, .avi, .3gp, etc.), sound (.mp3,. wav,. m4a, etc), Microsoft Word files (.doc, .docx, .rtf), Microsoft Excel (.xls, .xlsx), Microsoft PowerPoint (. ppt,. pptx), Text (. txt) and Portable Document Format (.pdf) to do the encryption and decryption.

Keyword*: Cryptography, Blowfish algorithm, database, security.*

1.1 Pendahuluan

Seiring dengan perkembangan teknologi dalam dunia bisnis, sistem basis data telah menjadi simbol dari salah satu bentuk aset yang paling berharga. Basis data telah menjadi kebutuhan di beberapa organisasi dan perusahaan komersial pada saat ini.

Basis data digunakan secara luas untuk berbagai bidang seperti bisnis, perbankan, pendidikan, kepegawaian, dan lain-lain. Dengan semakin luasnya penggunaan sistem basis data, perlindungan terhadap informasi yang disimpan dalamnya menjadi sangat diperlukan untuk melindungi dari berbagai macam ancaman diantaranya pembacaan data, manipulasi data dan perusakan data oleh pihak yang tidak berwenang. Ada beberapa tingkatan keamanan pada sistem basis data, diantaranya : keamanan sistem oprasi, keamanan sistem manajemen basis data, keamanan jaringan, dan keamanan segi manusia.

2.1 Landasan Teori

2.1.1 Kriptografi

2.1.1.1 Konsep Dasar Algoritma Kriptografi

Kriptografi (*cryptography)* merupakan ilmu penyimpanan pesan, data atau informasi secara aman. Secara etimologis kriptografi berasal dari bahasa yunani *krupto* berarti tersembunyi atau rahasia dan *grafh* artinya tulisan, sedangkan kriptografi menrut terminologinya dapat diartikan sebagai berikut :

1. Kriptografi adalah ilmu atau seni untuk mengamankan pesan. [Bruce Schneier, 1998]
2. Kriptografi adalah ilmu atau seni untuk menjaga kerahasiaan pesan dengan cara menyandikanya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. [Rinaldi Munir, 2006]
3. Kriptografi adalah ilmu dan seni untuk menjaga pesan ketika pesan dikirim dari suatu tempat ke tempat lain. [Dony Ariyus, 2008]

Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *cryptology*. Kriptografi bertujuan menjaga kerahasaiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat di ketahui oleh pihak yang tidak berhak. Dalam menjaga kerahaisaan data, kriptografi mentransformasikan data jelsa (*plaintext)* kedalam bentuk data sandi (*ciphertext)* yang tidak dapat dikenali.

Proses transformasi dari plainteks menjadi cipherteks disebut proses *encipherment* atau enkripsi (*encryption)*, sedangkan proses mentransformasikan kembali cipherteks menjadi plainteks disebut proses *decipherment* atau dekripsi (*decryption)*. Suatu pesan tidak disandikan sebagia *plaintext* ataupun dapat disebut juga sebagai *cleartext.* Proses yang dilakukan untuk mengubah plainteks ke dalam cipherteks disebut

encryption atau *encipherment.* Sedangkan proses untuk mengubah cipherteks kembali ke plainteks disebut *decryption* atau *decipherment*.

Kriptografi lebih dari enkripsi dan dekripsi saja.Namun juga memberikan komponen-komponen [Yusuf Kurniawan, 2004] sebagai berikut :

1. *Authentication* (keaslian), menjamin entitas yang berkomunikasi merupakan pihak yang berhak.
2. *Data confidentiality* (kerahasiaan data), melindungi dari pihak yang tidak berhak.
3. *Data integrity* (integritas data), menjamin data yang diterima sama persis dengan data yang dikirim, tidak mengandung modifikasi, tambahan, penghapusan dan sebagainya.
4. *Nonrepudiation* (anti penyangkalan), mencega pihak pengirim menolak untuk mengaku telah mengirim sebuah pesan.

Keamanan dari suatu sistem kriptografi (*cryptosystem*) biasanya terletak pada kerahasaiaan pada beberapa kunci yang dijadikan sebagai *ciphertext* pada algoritma kriptografi tersebut. Sistem kriptografi yang kuat memiliki kemungkinan jangkauan kunci yang sangat besar sehingga sistem ini tidak memungkinkan dipecahkan dengan mencoba semua kemungkinan kunci secara *bruteforce*.

Secara gatis besar kriptografi dibagi menjadi 2 jenis yaitu kriptografi klasik dan kriptografi modern. Perbedaan mendasar yang terdapat pada kedua jenis tersebut adalah pada kriptografi modern, algoritma kriptografi umumnya beroprasi pada mode-bit sehingga kriptanalis sangat sulit untuk memecahkan cipherteks tanpa mengetahui kuncinya, sedangkan kriptografi klasik beroprasi pada mode karakter, sehingga memungkinkan cipherteks dapat dipecahkan dengan muda, seperti penggunaan statistik kemunculan huruf pada bahasa tertentu, terkaan, ilustrasi dan sebagainya. Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya [Dony Ariyus, 2008] yaitu :

1. Algoritma Kriptografi Kunci Simetris

   Pada algoritma kriptografi ini, kunci yang digunakan dalam proses dekripsi dan enkripsi merupakan kunci yang sama. Berdasarkan pemrosesan bit, algoritma kunci simetris dibagi menjadi dua bagian, yaitu: algoritma cipher blok (*block cipher*) yang melakukan pemrosesan bit per-blok, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya dan algoritma cipher aliran (*stream cipher*) yang memperoses blok secara mengalir atau per-bit, rangkaian bit dienkripsi dan didekripsi bit per bit. Algoritma yang memakai kunci simetris di antaranya adalah Data Encryption Standard (DES), RC2, RC4, RC5, RC6, International Data Encryption Algorithm

(IDEA), Blowfish, One Time pad (OTP), A5 dan lain sebagainya. Dibawah ini diperlihatkan proses enkripsi/dekripsi kriptografi kunci simetris.

2. Algoritma Kriptografi Kunci Asimetris

Algoritma asimetris sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu:

1. Kunci umum (*public key*) : Kunci yang boleh semua orang tahu (dipublikasikan).
2. Kunci rahasia (*private key*) : Kunci yang dirahasiakan (hanya diketahui oleh satu orang).

Kunci-kunci tersebut berhubungan satu sama lain. Dengan kunci publik orang hanya dapat mengenkripsi pesan tetapi tidak dapat mendekripsinya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsi pesan tersebut. Algoritma yang memakai kunci simetris diantanya adalah Digital Signature Algoritma (DSA), RSA, Elliptic Curve Cryptography (ECC), Kriptografi Quantum, dan lain sebagainya.

3. Fungsi Hash

Fungsi Hash sering disebut dengan fungsi Hash satu arah (*one-way function*), *message diges, fingerprint,* fungsi kompresi dan *message authentication code* (MAC), merupkan satu fungsi matematika yang mengambil masukan panjang variabel dan mengubanya ke dalam urutan biner dengan panjang yang tetap. Fungsi Hash bisanya diperlukan bila ingin membuat sidik jadi dari suatu pesan. Sidik jadi pada pesan merupakan suatu tanda bahwa pesan tersebut benar-benar berasal dari orang yang di inginkan.

2.1.1.2 Algoritma Kriptografi

2.1.1.2.1 Algoritma Blowfish

Blowfish atau disebut juga *OpenPGP.Cipher.4* adalah algoritma kunci simetrik cipher blok dengan panjang blok tetap 64 bit dan menerapkan teknik kunci berukuran sembarang serta bebas lisensi dan dirancang pada tahun 1993 oleh Bruce Schneier untuk menggantikan DES (*Data Encryption Standard*). Algoritma blowfish dibuat untuk digunakan pada komputer yang mempunyai microprosesor besar (32-bit keatas dengan cache data yang besar).

Kriteria rancangan algoritma blowfish adalah sebabgai berikut :

1. Cepat, Blowfish melakukan enkripsi data pada microprocessor 32-bit dengan rate 26 *clock cycles* per byte.
2. *Compact,* Blowfish dapat dijalankan pada memory kurang dari 5 KB.
3. Sederhana, Blowfish hanya menggunakan oprasi yang sederhana, seperti: penamabahan, XOR, dan lookup tabel pada *operand* 32-bit.
4. Memiliki tingkan keamanan yang variatif, panjang kunci yang digunakan oleh blowfish bervariasi dan bisa sampai panjang miniman 32-bit, maksimal 448-bit, *Multiple* 8-bit, *default* 128-bit.

Namun, dalam penerapannya sering kali algoritma ini menjadi tidak optimal. Karena strategi implementasi yang tidak tepat. Algoritma blowfish akan lebih optimal jika digunakan untuk aplikasi yang tidak sering berganti kunci, seperti jaringan komunikasi atau enkripsi file otomatis.

2.1.1.2.2 Struktur Algoritma Blowfish

Blowfish merupakan blok cipher 64 bit dengan panjang kunci variabel. Algoritma ini terdiri dari dua bagian : *key expansion* atau perluasan kunci dan enkripsi data.

1. Key expansion

   Berfungsi merubah kunci (Minimum 32-bit, maksimum 448-bit) menjadi beberapa array subkunci (*subkey*) dengan total 4168 byte.
2. Enkripsi data

   Proses ini terdiri dari iterasi fungsi sederhana (*Feistel Network*) sebanyak 16 kali putaran. Setiap putaran terdiri dari permutasi key-dependent serta substitusi kunci dan data-dependent. Semua operasi merupakan penambahan (*addition*) dan XOR pada variable 32-bit. Operasi tambahan lainnya hanyalah empat penelusuran tabel (*table lookup*) array berindeks untuk setiap putaran.

2.1.1.2.3 Keamanan Blowfish

Sampai saat ini algoritma Blowfish belum ditemukan kelemahan yang berarti hanya adanya *weak* key dimana dua entri dari S-box mempunyai nilai yang sama. Blum ada cara untuk mengecek *weak key* sebelum melakukan *key* expansion, tetapi hal ini tidak berpengaruh terhadap hasil enkripsi.

Hasil enkripsi dengan algoritma Blowfish sangat tidak mungkin dan tidak praktis untuk di terjemahkan tanpa bantuan kunci. Samapai kini belim ada *cryptoanalyst* yang dapat membongkar pesan tanpa kunci yang di enkripsi dengan memakai bantuan algoritma Blowfish. Agar aman dari pembongkaran pesan maka dalam algoritmanya

harus menggunakan 16 putaran agar pesan tersebit tidak dapat dibongkar. Algoritma Blowfish pun cukup dapat digabingkan dengan algoritma enkripsi yang lain dalam pengenkripsian sebuah data untuk lebih menjamin isi dari data tersebut. Sehingga algoritma blowfish cukup ama jika ingin digunakan.

2.1.2 Basis Data

2.1.2.1 Pengertian Basis Data

Secara etimologis basis data terdiri dari dua kata yaitu basis dan data yang dapat diartikan sebagai markas atau gudang, tempat bersarang atau berkumpul. Data adalah representasi fakta dunia nyata yang mewakili suatu objek seperti manusia, barang dan sebagainya yang direkam dalam bentuk angka, huruf, simbol, teks, gambar, atau kombinasinya. Menurut pengertian lain Basis data (*database*) merupakan sekumpulan data yang saling terintegrasi satu sama lain dan terorganisasi berdasarkan sebuah skema atau struktur tertentu dan tersimpan pada sebuah hardware komputer. (M.Rudyanto Arief, 2005)

2.1.2.2 Database Management system (DBMS)

Database management system (DBMS) adalah konsep basis data yang menyimpan semua data dalam bentuk tabel=tabel. Sebuah tabel menyimpan informasi mengenai sebuah subjek tertentu. Dengan DBMS sebuah basis data akan dengan mudah dikelola walaupun jumlah data banyak dan sangat kompleks.

Pada prinsipnya DBMS terbagi menjadi 3 data yaitu :

1. Data Definition, mendefinisikan jenis data yang akan dibuat, cara relasi data, validasi data dan lainnya.
2. Data Manifulation, Data yang telah dibuat dan didefinisikan akan dilakukan beberapa pengerjaan, seperti sharing data, proses query dan lain sebagainya.
3. Data control, Pada bagian ini berhubungan dengan cara mengendalikan data, seperti siapa yang dapat melihat isi data, bagaimana data bisa digunakan oleh banyak user dan sebagainya.

2.1.2.3 Structure Query Language (SQL)

Structure Query Language (SQL) adalah salah satu bahasa generasi level ke-4 (4^{th} GL) yang awalnya dikembangkan oleh IBM di *San Jose Research Laboratory*. SQL merupakan bahasa basis data relasional yang terdiri atas sekumpulan perintah untuk mendefinisikan, manipulasi dan mengontrol data.

SQL sendiri terbagi atas 2 bagian, yaitu:

1. Data Definition Language (DDL)

   DDL adalah bahasa yang memiliki kemampuan untuk mendefinisikan data yang berhubungan dengan pembuatan dan penghapusan objek seperti tabel. Indeks, bahkan basis datanya sendiri. Misal CREATE, DROP dan ALTER.

2. Data Manipulation Language (DML)

   DML adalah bahasa yang berhubungan dengan proses manipulasi data pada tabel, record. Misalnya, INSERT, UPDATE, SELECT, dan UPDATE. DML terbagi atas dua tipe, yaitu :

   a. DML prosedural, dimana pengguan harus menspesifikasikan data apa yang di butuhkan dan bagaimana mendapatkan data tersebut.
   b. DML deklaratif atau non-prosedural DML, dimana pengguna hanya menspesifikasikan data yang dibutuhkan tanpa menspesifikasikan bagaimana cara mendapatkan data itu. DML jenis ini adalah DML yang secara umum dikenal, contohnya adalah *SQL Language.*

2.1.2.4 Keamanan Basis Data

Salah satu aspek yang terpentik dalam keamana basis data adalah proteksi terhadap pengaksesan, pembacaan informasi, pemodifikasian dan pengrusakan data oleh pihak yang tidak mempunyai kewenangan. Keamanan basis data juga berarti menjaga penyalahgunaan basis data baik secara sengaja, misalnya pengambilan data atau pembacaan data, pengubhan data dan penghapusan data oleh pihak yang tidak berwenang, maupun secara tidak sengaja, misalnya kerusakan selama transaksi, anomali yang disebebkan oleh akses basis data konkuren, anomali yang disebebkan oleh pendistirbusian data pada beberapa komputer dan logika error yang mengancam kemampuan transaksi untuk mempertahankan konsistensi basis data.

Persoalan keamanan basis data dapat di kategorikan menjadi beberapa tingkatan, yaitu :

1. Fisikal

   Keamanan level ini menyangkut keamanan yang berkaitan dengan dimana tempat sistem basis data berada. Tempat tersebut harus dilindungi secara fisik.

2. Manusia

   Setiap pengguna basis data harus diatur otoritasnya sedemikian rupa sehingga setiap pengguna hanya dapat mengakses data yang berhak diakases oleh pengguna yang bersangkutan.

3. Sistem Operasi

   Kelemahan pada sistem operasi ini memungkinkan pengaksesan data oleh pihak yang tidak berwenang, karena hampir seluru jaringan sistem basis data diakses jarak jauh.

4. Sistem Basis Data

   Sistem basis data yang digunakan harus menjamin setiap penggunaan basis data agar tidak melangar otoritas yang dimilikinya masing-masing. Penggunaan basis data hanya dapat memakai basis data sesuai wewenang yang dimiliki dan diatur oleh administator basis data.

3.1 Analisis Sistem

Analisis sistem adalah penguraian dari suatu sistem informasi yang utuh ke dalam bagian-bagian komponennya dengan maksud untuk mengidentifikasikan dan mengevaluasi permasalahan, hambatan dan kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikan dalam perancangan aplikasi yang akan dibuat.

3.1.1 Identifikasi Permasalahan

3.1.1.1 Permasalahan yang Timbul

Permasalahan yang akan timbul pada basis data adalah penyalahgunaan terhadap hak akses basis data sehingga dapat terjadi Pembacaan data, manipulasi data dan perusakan data oleh pihak yang tidak berwenang sehingga integrity data kurang terjaga.

3.1.1.2 Identifikasi Penyebab Masalah

Timbulnya suatu masalah itu dikarenakan adanya beberapa faktor yang terjadi dikarenakan cara penyimpanan data dilakukan secara utuh tanpa adanya pengkodean terhadap data sehingga data mudah dibaca dan dimengerti maksudnya.

3.1.1.3 Titik Keputusan

Dari dua uraian tersebut maka dapat ditarik suatu titik keputusan yakni bagai mana caranya mengamankan data yang disimpan di dalam basis data, penelitian ini memberkan suatu cara yakni dengan cara penerapan enkripsi dan dekripsi pada basis data.

3.1.2 Kebutuhan Perangkat

Berikut dibawah ini perangkat yang dapat mendukung dalam perancangan aplikasi yang akan dibuat, yaitu :

3.1.2.1 Perangkat Keras (Hardware)

Dalam hal ini perangkat keras yang dimaksud adalah komputer yang dibutuhkan untuk membangun serta mengimplementasikan sistem tersebut. Agar sebuah sistem dapat berjalan dengan baik dan mempunyai kemampuan yang memadai unutk sistem tersebut. Adapun perangkat keras yang digunakan untuk menjalankan aplikasi ini, mempunyai spesifikasi sebagai berikut :

a. Processor Intel Pentium dual-core T2390 1.86 GHz
b. RAM 3 GB
c. Harddisk 160 GB
d. Vga intel X3100

3.1.2.2 Perangkat Lunak (Software)

Sofware di sini merupakan software yang digunakan dalam pembuatan perangkat lunak yaitu Visual Basic 6.0

4.1 Hasil Penelitian dan Pembahasan

Setelah aplikasi dibuat dan berhasil dijalankan, maka dilakukan uji coba dengan beberapa sampel. Dari hasil pengujian, di dapat bahwa implementasi yang dilakukan di sistem operasi Windows berhasil. Semua jenis file yang telah diuji seperti file Microsoft SQL server (.mdf), Gambar (.jpg, .gif, .bmp, .png, dll), Video (.wmp, .mpeg, .mp4, .avi, .3gp, dll), Suara (.mp3, .wav, .m4a, dll), Microsoft Word (.doc, .docx, .rtf, .txt), Microsoft Excel (.xls, .xlsx), Microsoft PowerPoint (.ppt, .pptx), Text (.txt) dan *Portable Document Format* (.pdf) dapat dilakukan proses enkripsi dan dekripsi tanpa adanya perbahan terhadap file aslinya.

Dari hasil uji coba program diketahui bahwa sistem ini memilikin kelebihan dan kekurangan sebagai berikut :

1. Kelebihan Sistem
    a. Program ini dapat melakukan proses enkripsi dan dekripsi pada file sql, text, video, gambar, dokumen office dan pdf.
    b. Perbedaan ukuran file sebelum dan sesudah di enkripsi relative sama.
    c. Tidak ada perubahan extensi pada file yang dihasilkan dalam proses enkripsi.

2. Kekurangan sistem
    a. Sistem ini belum bisa mengenkrip file dengan besaran file lebih dari 32 Mb.
    b. Sebagian hasil enkripsi tidak bisa dibuka, tetapi dapat di dekripsi lagi.

5.1 Kesimpulan

Dari hasil analisis pada program enkripsi dan dekripsi, dapat ditarik kesimpulan sebagai berikut :

- Keamanan basis data dapat tercapai dengan cara mengimplementasikan algoritma blowfish kedalam suatu bahasa pemrograman sehingga dapat menerapan teknik kriptografi untuk pengamanan basis data dengan mengunakan algoritma blowfish. Penerapan ini sangatlah bermanfaat untuk menjaga kerahasiaan pada suatu file basis data dan file file lainya.
- Aplikasi ini dirancang untuk melakukan pengamanan basis data dengan cara melakukan enkripsi atau pengkodean data sehingga file basis data tidak dapat di attach ke software MS SQL Server dan file basis data dapat di gunakan kembali dengan caran melakukan porses dekripsi. Untuk proses enkripsi dan dekripsi harus menggunakan password, Password untuk enkripsi harus sama dengan password untuk dekripsi. Hasil file terenkripsi berupa file dalam bentuk ascii yang tidak dapat dibuka dengan aplikasi pembentuk, misalnya untuk dokumen word setelah proses enkripsi tidak dapat dikenali sebagai dokumen word dan data dalam dokumen tidak dapat dibaca lagi.

DAFTAR PUSTAKA

Arief, M.Rudyanto. *Pemrograman Basis Data Menggunakan Transact-SQL dengan Microsof SQL Server 2000,* Andi Offset, Yogyakarta, 2005

Ariyus, Dony. *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*, Andi Offset, Yogyakarta, 2008

Ratih, *Studi dan Implementasi Algoritma Blowfish Untuk Aplikasi Enkripsi dan Dekripsi File* (www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah1/Makalah1-077.pdf. Diakses 10 agustus 2011)

Rhee, Man Young. *Cryptography and Sesure Communications*, Singapore, McGraw-Hill Book Co.1994

Schneier, Bruce. *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)* (http://schneier.com Diakses 28 agustus 2011)

Suta. *Mengenal Visual Basic* (http://suta32.googlepages.com/suta32-Bab1-MengenalVisualBasic6.0.pdf. Diakses 26 september 2011)