IMPLEMENTASI ENKRIPSI BASIS DATA BERBASIS WEB DENGAN ALGORITMA STREAM CIPHER RC4

Aditya Eka Arifyanto
Jurusan Teknik Informatika, Fakultas ilmu Komputer
Universitas Dian Nuswantoro

Distributor Sepatu Ramayana Semarang adalah suatu perusahaan yang bergerak dalam bidang distribusi sepatu di kota Semarang. Sebagai suatu perusahaan, tentunya Distributor Sepatu Ramayana memiliki sebuah aplikasi sistem yang digunakan dalam mengolah data transaksi, kepegawaian, dan lainnya yang terhubung dengan suatu basis data. Keamanan basis data merupakan aspek yang sangat penting dari suatu sistem informasi. Sebuah informasi umumnya hanya ditujukan untuk golongan tertentu. Oleh karena itu sangat penting untuk bagi perusahaan ini untuk mencegah adanya kebocoran basis data agar informasi yang ada didalamnya tidak jatuh ke orang yang tidak berkepentingan. Salah satu cara untuk menjaga keamanan basis data tersebut adalah menggunakan teknik enkripsi. Penulis menggunakan metode enkripsi stream cipher RC4 karena metode tersebut memiliki kelebihan dalam kecepatan pemrosesan dan tingkat keamanan yang cukup tinggi. Dengan penggunaan metode enkripsi stream cipher untuk menjaga keamanan basis data, informasi yang terdapat dalam basis data tersebut hanya dapat dilihat oleh orang yang memiliki kepentingan dengan informasi tersebut.

***Kata kunci** : Basis data, Kriptografi, RC4.*

1. PENDAHULUAN

A. Latar Belakang

Di era modern ini, hampir seluruh instansi, perusahaan, dan perkantoran telah menerapkan penggunaan sistem basis data dalam mengolah dan menyimpan informasi. Saat ini, keamanan terhadap data yang tersimpan dalam basis data sudah menjadi persyaratan mutlak. Namun, bukan berarti data – data tersebut aman dari kebocoran informasi. 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. Diperlukan adanya suatu sistem yang dapat membatasi hak akses maupun mengamankan informasi yang terkandung dalam data tersebut tanpa campur tangan administrator basis data.

Kriptografi adalah suatu teknik penyembunyian informasi yang terkandung pada suatu data dengan cara enkripsi. Penerapan kriptografi pada Tugas Akhir 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 adalah algoritma kriptografi simetris dan bersifat *stream cipher* sehingga data yang telah di enkripsi (ciphertext) akan memiliki ukuran yang samadengan data asli (plaintext), keuntungan lain algoritma stream cipher adalah proses komputasi yang lebih cepat disbanding algoritma lainnya.

Berdasarkan informasi diatas, penulis merancang sebuah sistem yang menerapkan metode enkripsi simetris dalam secure login aplikasi yang diimplementasikan dalam Tugas Akhir dengan judul “**Implementasi Enkripsi Basis Data Berbasis Web Dengan Algoritma Stream Cipher RC4**”.

B. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, dapat diambil rumusan masalah bagaimana merancang suatu sistem enkripsi basis data pada data login yang dapat membantu keamanan aplikasi program dan database.

C. Tujuan Penulisan

1) Untuk membuat system keamanan login aplikasi program dengan menggunakan enkripsi.

2) Mengimplementasikan teknik kriptografi kedalam sebuah aplikasi sistem.

D. Manfaat Penelitian

1. Membantu perusahaan dalam menjaga keamanan sistem

aplikasi dan database yang ada pada perusahaan tersebut.

2. Menambah integritas database itu sendiri sehingga dapat mendeteksi adanya penambahan, pengubahan, penghapusan data yang tidak sesuai dengan hak akses.

2. BAHAN DAN METODE

Penelitian perancangan aplikasi sistem informasi ini dilakukan berdasarkan permasalahan yang telah diuraikan sebelumnya, adapun tahapan – tahapan yang akan dilalui adalah sebagai berikut :

1. Studi Literatur

   Mengumpulkan beberapa jurnal, *paper*, dan penelitian terkait sebelumnya (skripsi) dengan metode *Library Research* dengan mengunjungi perpustakaan dan meminjam buku pendukung dan beberapa skripsi dengan penelitian yang sama sebelumnya serta mengunduh jurnal – jurnal literatur dari jurnal lokal ataupun internasional yang mendukung. Dan hasilnya telah dikemukakan pada bab sebelumnya. Dengan menggunakan metode ini mempengaruhi hampir seluruh bagian dalam penelitian ini.

2. Observasi

   Karena pada penelitian ini berupa studi pustaka yang memiliki obyek nyata untuk diteliti maka kunjungan ke objek terkait dilakukan untuk mengumpulkan data berupa :

   1. Data dan fakta Distributor Sepatu Ramayana
   2. Informasi sistem login aplikasi yang digunakan
   3. Alur kerja sistem login kedalam aplikasi

3. Pengembangan Sistem

   Metode perancangan sistem yang digunakan dalam tugas akhir ini adalah dengan menggunakan model proses perancangan perangkat lunak *Prototyping* melalui paradigma/pendekatan berorientasi objek yang dimodelkan menggunakan *Unified Modeling Language* (UML).

   Metode *Prototyping* merupakan metode yang menyajikan gambaran yang lengkap tentang

sistemnya, metode ini banyak digunakan karena pengembang mungkin tidak memiliki kepastian terhadap efisiensi algoritma, kemampuan penyesuaian dari sebuah sistem operasi, atau bentuk-bentuk yang harus dilakukan oleh interaksi manusia dengan mesin sehingga paradigma *prototyping* ini merupakan pendekatan terbaik yang ditawarkan.

Paradigma *prototyping* dimulai dengan pengumpulan kebutuhan. Pengembang dan pelanggan bertemu untuk mendefinisikan obyektif kebutuhan dari perangkat lunak, mengidentifikasi segala kebutuhan yang diketahui, dan area garis besar dimana definisi lebuh jauh merupakan keharusan yang kemudian dilakukan perancangan kilat. Perancangan kilat berfokus pada penyajian dari aspek-aspek perangkat lunak tersebut yang akan terlihat bagi pelanggan. Perancangan kilat membentuk konstruksi sebuah *prototype. Prototype* tersebut dievaluasi oleh pelanggan dan digunakan untuk menyaring kebutuhan perancangan perangkat lunak. Iterasi terjadi pada saat *prototype* dirancang untuk memenuhi kebutuhan pelanggan dan pada saat yang sama memungkinkan pengembang untuk memahami apa yang akan dilakukan selanjutnya.

Keunggulan dari penggunaan paradigma *prototyping* adalah :

1. Pengembang dapat bekerja lebih baik dalam menentukan kebutuhan
2. Lebih menghemat waktu dalam pengembangan sistem
3. Penerapan menjadi lebih mudah karena pemakai mengetahui apa yang diharapkannya.

3. HASIL DAN ANALISA

A. Algoritma RC4

Algoritma kriptografi Rivest Code 4 (RC4) merupakan salah satu algoritma kunci simetris dibuat oleh RSA Data Security Inc (RSADSI) yang berbentuk stream chipper. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu : Rivest Shamir Adleman). RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte. Tabel ini

digunakan untuk generasi yang berikut dari pseudo random yang menggunakan XOR dengan plainteks untuk menghasilkan cipherteks. Masing-masing elemen dalam tabel saling ditukarkan minimal sekali.

B. Langkah – langkah algoritma RC4

RC4 memiliki sebuah S-Box, S0, S1, …, S255 yang berisi permutasi dari bilangan 0 sampai 255, dan permutasi merupakan fungsi dari kunci K dengan panjang yang variable.

1. Inisialisasi S-Box

   a. Isi S-Box secara berurutan, yaitu S0=0,S1=1, …, S255=255.

   b. Lakukan padding kunci K sehingga panjang kunci K = 256

   c. Lakukan pertukaran dan pengisian pada S-Box dengan kunci K, sebagai berikut :

      j = 0

      for i = 0 to 255

      j = (j + S_i + K_i) mod 256

      swap S_i dan S_j

   Fungsi swap merupakan fungsi yang menukarkan nilai S ke-i dengan nilai S ke-j.

2. Proses enkripsi atau dekripsi RC4

   i = 0

   j = 0

   for idx = 0 to len-1

   i = (i + 1) mod 256

   j = (j+ S_i) mod 256

   swap S_i dan S_j

   t = (S_i + S_j) mod 256

   k = S_t

   $buff_{idx}$ = k XOR $buff_{idx}$

   Keterangan :

   1. Buff merupakan pesan yang akan dienkripsi atau dekripsi
   2. Len merupakan panjang dari buff yang berisi pesan yang telah dienkripsi atau dekripsi.

4. PEMBAHASAN

	id	key
	1	adityasniper

Check All / Uncheck All With selected:

Tabel x.x Master Key untuk proses enkripsi dan dekripsi

Tabel di atas merupakan tabel key atau kunci utama dalam sistem enkripsi dan dekripsi. Panjang data kunci ini mempengaruhi kekuatan dari sistem enkripsi data. Semakin panjang kunci yang digunakan, maka semakin kuat sistem keamanan tersebut dari serangan.

	id	namalengkap	username	alamat	nohp	password	level
	24	Annisa Widya Paramitha	annisa	Jl. Bukit Barisan DVI/11	1234567890	¿Ã¯¬é¿Fûy'à	user
	26	Sulaiman	leman	jl.mt haryono semarang	2147483647	£*] ¶ß.Bä	user
	28	Aditya E A	SU	Jl. Bukit Barisan DVI/11	08564043214 5	¼@$‡ªU	superuser
	30	Reynaldi Arwana	tukul	trans 7 jakarta	758490375849	®=G ›¤	superuser
	31	Vega Darmawanti	vega	Jakarta Pusat	84933892929	jlQ5ræx›	admin

Check All / Uncheck All With selected:

Tabel x.x Tabel User yang telah berhasil dienkripsi passwordnya

Tabel diatas adalah gambar dari tabel user yang telah berhasil dienkripsi. Password yang tersimpan dalam database yang biasanya dapat dibaca sebelum di enkripsi, kini sulit untuk dimengerti oleh orang yang tidak memiliki key untuk mendekripsikannya.

5. KESIMPULAN

1. Program aplikasi enkripsi basis data ini akan membantu menjaga keamanan dan kerahasiaan informasi yang tersimpan dalam sistem basis data yang terdapat pada Distributor Sepatu Ramayana Semarang.
2. Penggunaan algoritma RC4 cocok diterapkan pada penerapan enkripsi sistem basis data karena cukup kuat untuk menjaga keamanan basis data.

6. SARAN

Adapun saran yang penulis usulkan untuk melanjutkan pengembangan sistem ini adalah:

1. Aplikasi ini sebaiknya diberikan *maintenance* secara teratur agar jika terdapat bug di dalam sistem dapat segera diatasi.
2. Memberikan ukuran server yang besar karena menjaga performa sistem saat digunakan *user*.
3. Dapat dikembangkan lebih luas lingkupnya, tidak hanya enkripsi pada password user saja. Namun dapat diimplementasikan pada file –

file yang berisi informasi penting agar tidak dapat dimengerti orang lain.

7. DAFTAR PUSTAKA

[1] Ruri Hartika Zain, S.Kom, M.Kom. *Perancangan Dan Implementasi Cryptography Dengan Metode Algoritma Rc4 Pada Type File Document Menggunakan Bahasa Pemrograman Visual Basic 6.0*. Dosen Fakultas Ilmu Komputer

[2] Rohmat Sobar[1], Yoyok Andoyo[2], Noni Juliasari[3], Galuh Dian Maulana[4]. 2005. *Pengamanan Data Sistem Billing Warnet Dengan Menggunakan RC4 Stream Cipher*. Magister Ilmu Komputer, Fakultas Ilmu Komputer, Universitas Indonesia.

[3] Suhendra, Ari. 2012. *Analisis dan Implementasi Enrkipsi Basis Data dengan Algoritma Kriptografi Blowfish*. Stimik Amikom Yogyakarta.

[4] Rudyanto, Arief M. 2007. *Sistem Basis Data*. Stimik Amikom Yogyakarta.

[5] Rudyanto, Arief M. 2007. *Modul Pratikum Sistem Basis Data Dengan SQL Server 2000*. Stimik Amikom Yogyakarta.