

IMPLEMENTASI RC4 STREAM CIPHER UNTUK KEAMANAN BASIS DATA

Wachyu Hari Haji¹, Slamet Mulyono²

^{1,2}Jurusan Sistem Informasi, Fakultas Ilmu Komputer, Universitas Mercu Buana Jakarta
Jalan Meruya Selatan No. 1 Jakarta Barat 11610
E-mail:wahyuhari@gmail.com,slamet_mulyono@yahoo.com

ABSTRAK

Kemajuan teknologi yang sangat cepat mendorong setiap instansi untuk tetap mengikuti perkembangan teknologi dan terus meningkatkan kemampuannya dalam mengelola data-data dan informasi yang lebih aman, akurat, dan efisien yang dibutuhkan suatu instansi. Salah satu hal terpenting dalam komunikasi menggunakan komputer dan jaringan komputer adalah untuk menjamin keamanan pesan, data, ataupun informasi dalam proses pengiriman atau penyimpanan data, sehingga menjadi salah satu pendorong munculnya teknologi kriptografi. Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy. Penggunaan algoritma RC4 Stream Cipher karena cukup mudah untuk digunakan secara luas pada beberapa aplikasi dan algoritmanya sudah dinyatakan cukup aman untuk diterapkan. Ada banyak model dan metode enkripsi, salah satu di antaranya adalah enkripsi dengan algoritma Rivest Code 4 (RC4). Hasil penelitian ini adalah penggunaan program Enkripsi RC4 Stream Cipher dengan jumlah karakter asli (plaintext) berhasil di enkripsi sama dengan jumlah karakter hasil enkripsi (chiphertext) sehingga data yang di input akan di simpan pada database dalam keadaan terenkripsi sehingga keamanan dan kerahasiaan datanya dapat terjaga.

Kata kunci: Cryptography, Encryption, Decryption, RC4

1. PENDAHULUAN

Kemajuan teknologi yang sangat cepat mendorong setiap instansi untuk tetap mengikuti perkembangan teknologi dan terus meningkatkan kemampuannya dalam mengelola data-data dan informasi yang lebih aman, akurat, dan efisien yang dibutuhkan suatu instansi. Untuk itu dibutuhkan suatu sistem informasi yang mendukung kebutuhan informasi yang akan sangat membantu sebuah manajemen instansi baik dalam menciptakan efisiensi dan efektifitas kerja instansi itu sendiri, maupun dalam meningkatkan pelayanan kepada masyarakat. Dengan suatu sistem informasi maka pengolahan data akan lebih mudah dan efisien.

Salah satu hal terpenting dalam komunikasi menggunakan komputer dan jaringan komputer adalah untuk menjamin keamanan pesan, data, ataupun informasi dalam proses pengiriman atau penyimpanan data, sehingga menjadi salah satu pendorong munculnya teknologi kriptografi. Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan authenticity (perlindungan terhadap pemalsuan dan perubahan informasi yang tidak diinginkan).

Melihat permasalahan yang ada menjadi pertimbangan bagi penulis untuk memilih sebuah algoritma kriptografi yang akan digunakan dalam penyusunan tugas akhir ini, penulis memilih algoritma RC4 Stream Cipher karena dapat di implementasikan untuk pengamanan database. Algoritma RC4 Stream Cipher ini cukup mudah untuk dijelaskan dan sudah digunakan secara luas

pada beberapa aplikasi dan algoritmanya sudah dinyatakan cukup aman untuk diterapkan. Ada banyak model dan metode enkripsi, salah satu di antaranya adalah enkripsi dengan algoritma Rivest Code 4 (RC4).

2. SECURITY

Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus. Selain itu, pastikan bahwa user dalam jaringan memiliki pengetahuan yang cukup mengenai keamanan dan pastikan bahwa mereka menerima dan memahami rencana keamanan yang anda buat. Jika mereka tidak memahami hal tersebut, maka mereka akan menciptakan lubang (hole) keamanan pada jaringan Anda.

3. KRIPTOGRAFI

Kriptografi merupakan seni dan ilmu menyembunyikan informasi dari penerima yang tidak berhak (unauthorized persons). Kata cryptographi berasal dari kata Yunani kryptos (tersembunyi) dan graphein (menulis). Cryptanalysis adalah aksi untuk memecahkan mekanisme kriptografi dengan cara mendapatkan plaintext atau kunci dari ciphertext yang digunakan untuk mendapatkan informasi berharga kemudian

mengubah atau memalsukan pesan dengan tujuan untuk menipu penerima yang sesungguhnya.

Encryption adalah mentransformasi data kedalam bentuk yang tidak dapat terbaca tanpa sebuah kunci tertentu. Tujuannya adalah untuk meyakinkan privasi dengan menyembunyikan informasi dari orang-orang yang tidak ditujukan, bahkan mereka yang memiliki akses ke data terenkripsi. Dekripsi merupakan kebalikan dari enkripsi, yaitu transformasi data terenkripsi kembali ke bentuknya semula.

4. ENKRIPSI-DEKRIPSI

Enkripsi-dekripsi merupakan salah satu fungsi dasar yang disediakan kriptografi adalah sebuah proses penyandian data atau pesan terbuka menjadi pesan rahasia (ciphertext). Ciphertext inilah yang nantinya akan dikirimkan melalui saluran komunikasi terbuka. Pada saat ciphertext diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan.

Algoritma kriptografi (Cryptographic Algorithm) atau sering disebut chiper merupakan fungsi matematika yang digunakan untuk proses enkripsi dan dekripsi dimana proses enkripsi dan dekripsi diatur oleh salah satu atau beberapa kunci kriptografi. Secara umum, kunci-kunci yang digunakan untuk pengenkripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan. Secara matematis proses enkripsi dan dekripsi dapat ditulis (Trappe, 2002):

$$Ek(M) = C \text{ (Proses enkripsi)}$$

$$Dk(C) = M \text{ (Proses dekripsi)}$$

Dimana: E = Proses enkripsi

K = Kunci

M = Teks asli

C = Teks terenkripsi

D = Proses dekripsi

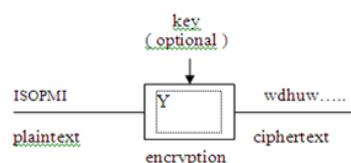
Pada saat proses enkripsi, pesan (M) akan di sandikan dengan menggunakan kunci enkripsi (K) menjadi sandi yang tidak dimengerti (C) sedangkan pada proses dekripsi, sandi yang tidak dimengerti (C) tersebut di uraikan dengan menggunakan kata kunci dekripsi (K) sehingga menghasilkan pesan (M) yang sama seperti pesan sebelumnya.

5. CIPHER

Secara umum dalam proses enkripsi-dekripsi dikenal dua macam cipher berdasarkan cara kerja penyandiannya, yaitu Stream cipher adalah suatu sistem dimana proses enkripsi dan dekripsinya dilakukan dengan cara bit per bit. Pada sistem ini aliran bit kuncinya dihasilkan oleh suatu pembangkit bit acak. Aliran kunci ini dikenakan operasi XOR dengan aliran bit-bit dari plaintext untuk menghasilkan aliran bit-bit ciphertext (Kurniawan, 2004).

Pada proses dekripsi aliran bit ciphertext dikenakan operasi XOR dengan aliran bit kunci yang identik untuk menghasilkan plaintext. Keamanan dari sistem ini tergantung dari pembangkit kunci, jika pembangkit kunci menghasilkan aliran bit-bit 0 maka ciphertext yang dihasilkan akan sama dengan plaintext, sehingga seluruh operasi akan menjadi tidak berguna oleh karena itu diperlukan sebuah pembangkit kunci yang dapat menghasilkan aliran bit-bit kunci yang acak dan tidak berulang.

Semakin acak aliran kunci yang dihasilkan oleh pembangkit kunci, maka ciphertext akan semakin sulit dipecahkan. Contoh stream cipher adalah RC4, Seal, A5, Oryx, dll. Algoritma kriptografi aliran (Stream Cipher) dapat dilihat seperti pada gambar di bawah ini:



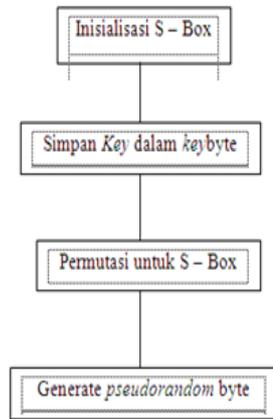
Gambar 1 Skema Enkripsi Stream Cipher

6. ALGORITMA RC4 STREAM CIPHER

Algoritma RC4 merupakan salah satu algoritma kunci simetris berbentuk stream cipher yang memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah byte atau bahkan bit (byte dalam hal RC4). Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses atau menambahkan byte tambahan untuk mengenkrip (Sukmawan, 1998).

RC4 mempunyai sebuah S-Box, S_0, S_1, \dots, S_{255} , yang berisi permutasi dari bilangan 0 sampai 255. Menggunakan dua buah indeks yaitu i dan j di dalam algoritmanya. Indeks i digunakan untuk memastikan bahwa suatu elemen berubah, sedangkan indeks j akan memastikan bahwa suatu elemen berubah secara random. Intinya, dalam algoritma enkripsi metode ini akan membangkitkan pseudo random byte dari key yang akan dikenakan operasi Xor terhadap plaintext untuk menghasilkan ciphertext.

Dan untuk menghasilkan plaintext semula, maka ciphertext nya akan dikenakan operasi Xor terhadap pseudo random bytenya. Berikut ini akan diberikan sebuah bagan yang menggambarkan rangkaian proses yang dijalankan untuk mengenkripsi atau mendekripsi data



Gambar 2. Rangkaian Proses RC4 Stream Cipher

7. BASIS DATA

Basis data adalah kumpulan data yang saling berhubungan yang disimpan secara bersama sedemikian rupa dan tanpa pengulangan atau redundansi yang tidak perlu, sehingga dapat digunakan untuk memenuhi berbagai kebutuhan (Fathansyah, 1999:2). Tujuan dari basis data itu sendiri adalah untuk menyimpan informasi yang ada secara tepat serta informasi yang telah disimpan tersebut dapat diambil dengan cepat dan efisien diwaktu yang akan datang sesuai dengan kebutuhannya.

Perancangan basis data merupakan hal yang sangat penting, segala macam data yang akan diolah harus dicatat, disimpan kemudian diolah menjadi informasi yang dibutuhkan. Kesulitan dalam merancang basis data adalah bagaimana merancang sehingga basis data agar terus konsisten dan dapat digunakan untuk pemenuhan keperluan saat ini maupun dimasa yang akan datang. Dalam merancang suatu basis data diperlukan pendekatan dengan metode konseptual yang menggunakan data relasional, dimana dapat menggunakan diagram keterhubungan entitas.

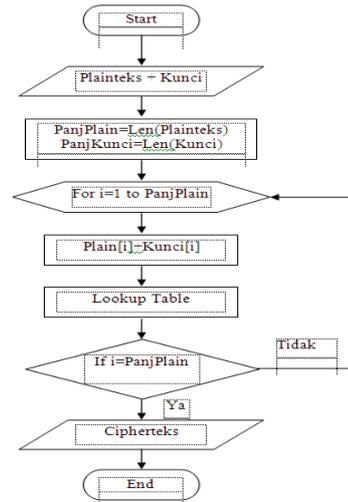
Untuk tahap desain database secara umum, yang perlu dilakukan oleh analis adalah mengidentifikasi terlebih dahulu file-file yang diperlukan oleh sistem informasi. File-file database yang dibutuhkan oleh sistem dapat dilihat pada desain model yang digambarkan dalam bentuk diagram arus data. Langkah-langkah desain database secara umum adalah dengan menentukan kebutuhan file database untuk sistem baru dan menentukan parameter dari file database.

Setelah file-file yang dibutuhkan telah dapat ditentukan, maka parameter dari file selanjutnya juga dapat ditentukan. Parameter ini meliputi: Tipe dari file: file induk, file transaksi, file sementara dan lain sebagainya, Media file: hard disk, diskette atau pita magnetic, Organisasi dari file: apakah file tradisional (file urutan, ISAM atau file akses langsung) atau organisasi database (struktur

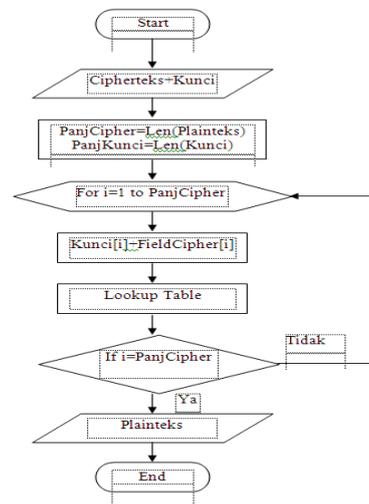
berjenjang jaringan atau hubungan). Field kunci dari file.

8. FLOWCHART ENKRIPSI-DEKRIPSI RC4 STREAM CIPHER

Diagram Flowchart ini digunakan untuk mendesain dan merepresentasikan program. Sebelum pembuatan program, fungsinya adalah mempermudah programmer dalam menentukan alur logika program yang akan dibuat. Sesudah pembuatan program fungsinya adalah untuk menjelaskan alur program kepada orang lain atau user



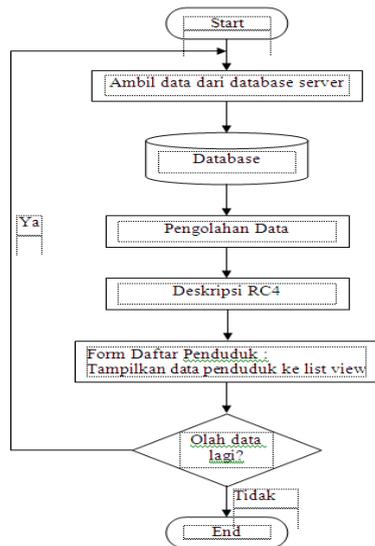
Gambar 3. Flowchart Enkripsi RC4



Gambar 4. Gambar Flowchart Enkripsi RC4

Perancangan Modul Dekripsi

Pada rancangan ini hampir sama dengan rancangan modul enkripsi hanya saja pada rancangan modul ini proses dekripsi dilakukan pada saat user melakukan edit data penduduk melalui form data diri yang di ambil dari database yang sudah di enkripsi



Gambar 5. Flowchart Deskripsi RC4

9. PENGUJIAN DAN ANALISA LINIERITAS

Pengujian ini dilakukan untuk mengetahui panjang dari simbol yang dihasilkan dari proses enkripsi-deskripsi menggunakan metode RC4 Stream Cipher dan membandingkannya dengan panjang teks aslinya apakah panjangnya sama dengan panjang karakter yang dikirimkan atau tidak. Dikatakan linier jika panjang hasil enkripsi sama dengan panjang karakter teks aslinya. Berikut ini adalah gambar hasil simbol enkripsi-deskripsi RC4 Stream Cipher dan untuk lebih jelasnya dapat dilihat pada tabel hasil enkripsi-deskripsi dibawah ini:

Tabel 1. Pengujian Panjang Karakter Teks

Keterangan	Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah Karakter Hasil
No.KTP	3671131205830004	16	8Z0Ú0¼Jcc~0H8m"É	16
Nama Lengkap	WACHYU HARI	14	Xu aU[00Q4X0	14
Jenis Kelamin	Laki-Laki	9	G0_ Å0!!	9
Gol. Darah	O	1	D	1
Tempat Lahir	WONOGIRI	10	00-hAS0 0	10

10. KESIMPULAN

Dari hasil perancangan dan pembuatan program enkripsi database pada aplikasi dengan menggunakan algoritma RC4 Stream Cipher ini, maka dapat diambil kesimpulan sebagai berikut:

1. Enkripsi RC4 Stream Cipher ini dapat diimplementasikan pada Aplikasi dengan menggunakan bahasa pemrograman visual basic 6.0 dan database Mysql.
2. Pada Program Enkripsi RC4 Stream Cipher ini jumlah karakter asli (*plaintext*) yang berhasil di enkripsi sama dengan jumlah karakter hasil enkripsi (*chipertext*).
3. Data yang di input akan di simpan pada database dalam keadaan terenkripsi sehingga keamanan dan kerahasiaan datanya dapat terjaga.

DAFTAR PUSTAKA

- Andi, Offset. (2003). Memahami Model Enkripsi & Security Data. Wahana Komputer Semarang, Yogyakarta.
- Ariyus, Doni. (2008). Pengantar Ilmu Kriptografi (Teori, Analisis, dan Implementasi). Yogyakarta : Andi
- B. Sukmawan, (1998). RC4 Stream Cipher. <http://www.bimacipta.com/rc4.htm>, diakses 23 November 2011 20.47 WIB
- Fauzan, Firda. (2008). Pengamanan Transmisi Hasil dan Data Query Basis Data dengan Algoritma Kriptografi RC4. Bandung
- Haller N., Metz C., Nesser P., Straw M., (1998), A One-Time Password System, Request for Comments 2289 (<http://www.rfc-editor.org>)
- Ir. Fathansyah, (1999). Basis Data, Informatika, Bandung
- Kristianto, Andri. (2003). Keamanan Data pada Jaringan Komputer. Gava Media, Yogyakarta.
- Kurniawan, Yusuf. (2004). Kriptografi: Keamanan internet dan jaringan komunikasi. Informatika Bandung, Bandung.
- Menezes, Alfred J.; Van Oorschot, Paul C.; Vanstone, Scott A., (1997), Handbook of Applied Cryptography, CRC Press.
- Munir, Rinaldi. (2006). Kriptografi. Informatika, Bandung.
- Pressman, Roger S. (2002). Rekayasa Perangkat Lunak Pendekatan Pratisi. Andi, Yogyakarta
- Stalling, William, (1995), Network and International Security Principles and Practice, Prentice Hall, New Jersey.
- Silberschatz, Korth, Sudarshan. (2002). Database System Concepts, 4rd edition, McGraw-Hill.
- Scheier, Bruce, 1993, Applied Cryptography: Protocols, Algorithms & Source Code in C, John Wiley & Sons Inc