**semanTIK**, Vol.2, No.1, Jan-Jun 2016, pp. 59-64
ISSN : 2502-8928 (Online)


# APLIKASI SISTEM KEAMANAN BASIS DATA DENGAN TEKNIK KRIPTOGRAFI RC4 *STREAM CIPHER*

**Jumrin*[1], Sutardi[2], Subardin[3]**
[*1,2,3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kendari
e-mail : ***[1]jumrin111@gmail.com**, [2]sutardi_hapal@yahoo.com, [3]mail.bardin@gmail.com

**Abstrak**

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 bagi suatu perusahaan untuk mencegah adanya kebocoran basis data agar informasi yang ada didalamnya tidak jatuh ke orang yang tidak berkepentingan. Teknik kriptografi merupakan salah satu alternatif solusi yang dapat digunakan dalam pengamanan basis data. Salah satu cara untuk menjaga keamanan basis data tersebut adalah menggunakan teknik enkripsi.

Metode yang digunakan untuk mengamankan basis data adalah dengan 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. Metode RC4 (*Rivest Code*) *Stream Cipher* merupakan salah satu algoritma kunci simetris berbentuk *stream chipper* yang memproses unit atau *input* data, pesan ataupun informasi.

Hasil penelitian ini menunjukan bahwa data pada tabel basis data dapat terenkripsi atau *ciphertext*, serta proses enkripsi dan dekripsi yang jauh lebih cepat dan memiliki tingkat keamanan yang tinggi.

**Kata kunci**— Kriptografi, *RC4 Stream Cipher*, Enkripsi, Dekripsi

***Abstract***

*Database security is a very important aspect in an information system. A specific information is generally addressed to specific group. Therefore it is an important matter for a company to prevent information leak from a database so that the information contained in it does not fall to unauthorized party. Cryptography is an alternate solution that can be used to secure a database. One method that can be used to secure a database is by using encryption.*

*The method used to secure a database is the RC4 Stream Cipher encryption because the method has advantages in processing speed and high security level. By using Stream Cipher encryption method to secure a database, the information contained in it can only be accessed by authorized party. RC4 (Rivest code) Stream Cipher method is one of symmetric key algorithm in form of Stream Cipher that process unit or data input, message, or information.*

*Research results show that a data in a database table can be encypted. The encryption and decryption process are faster and have high security level.*

***Keywords****— Cryptography, RC4 Stream Cipher, Encryption, Decryption*

## 1. PENDAHULUAN

Keamanan pada basis data telah menjadi kebutuhan yang penting pada suatu perusahaan. Kebutuhan ini timbul dari semakin banyaknya ancaman terhadap data sensitif yang terdapat pada basis data. Teknik kriptografi merupakan salah satu alternatif solusi yang dapat digunakan dalam pengamanan basis data. Akan tetapi,

pengembangan strategi kriptografi pada basis data membutuhkan banyak pertimbangan. data, mencakup analisis lingkungan, desain solusi dan persoalan persoalan yang ditemui dalam menentukan desain pengamanan basis data [1].

Penelitian ini didasarkan pada penelitian sebelumnya mengenai enkripsi pada basis data. Salah satu penelitian sebelumnya yang berjudul "*Analisis Dan Implementasi Enkripsi Basis Data Dengan Algortima Kriptografi Blowfish*", yang dilakukan oleh [2] yang pada penelitian tersebut menggunakan metode enkripsi *Blowfish* yang merupakan metode enkripsi yang bersifat 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. 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. Pada penelitian tersebut membuat sebuah aplikasi dengan mengunakan visual basic 6.0 yang mana bisa mengenkripsi *file* sql, text, video, gambar, dokumen office dan pdf. Sistem ini belum bisa mengenkrip *file* dengan besaran *file* lebih dari 32 Mb. Sebagian hasil enkripsi tidak bisa dibuka, tetapi dapat di dekripsi lagi [2].

Kemudian penelitian berikutnya berjudul "*Implementasi Algoritma Caesar Cipher Dan Hill Cipher Pada Database Sistem Inventori TB Mita Jepara*" yang dilakukan oleh [1]. Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Ini adalah algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga *Caesar Cipher*), untuk menyandikan pesan yang ia kirim kepada para gubernurnya. Caranya adalah dengan mengganti. *Hill Cipher* diperkenalkan pertama kali pada tahun 1929 oleh Letser S.Hill. Proses enkripsi dan dekripsi pada *Hill Cipher* menggunakan oprasi perkalian matriks atas ring $Z26$. Ide dasar dari *Hill* adalah untuk membuat kombinasi linier dari *plaintext* untuk mendapatkan *ciphertext*. Kunci yang digunakan berupa matriks persegi $Z26$ yang determinan-nya *invertibel* pada $Z26$. *Hill Cipher* termasuk dalam salah satu kripto sistem poli alfabetik, artinya setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter alfabet. *Cipher* ini ditemukan pada tahun 1929 oleh Lester S. Hill. Hasil dari penelitian dengan mengunakan algoritma *Caesar Cipher* dan *Hill Cipher* adalah dengan melihat hasil enkripsi *database* sistem inventori TB Mita Jepara. Hasil *output* yang didapat kolom (*field*) persediaan barang pada invetori TB Mita Jepara dapat terenkripsi [1].

Basis data merupakan tempat penyimpanan data penting yang dibutuhkan untuk menjamin kelancaran aktivitas suatu perusahaan. Data penting dan vital yang tersimpan pada basis data seringkali menjadi target empuk bagi para penyerang. Serangan yang terjadi dapat dilakukan oleh pihak luar (*hacker*) maupun pihak dalam (pegawai yang tidak puas). Selama ini, mekanisme pengamanan basis data diimplementasikan dengan menggunakan kontrol akses terhadap basis data tersebut. Akan tetapi, dengan berkembangnya penggunaan jaringan untuk pertukaran data, diperlukan strategi pengamanan yang lebih kuat daripada sekedar mekanisme control akses. Salah satu cara untuk mengamankan data pada basis data adalah dengan menggunakan teknik kriptografi yang diterapkan pada data tersebut [1].

## 2. METODE PENELITIAN

### 2.1 Kriptografi

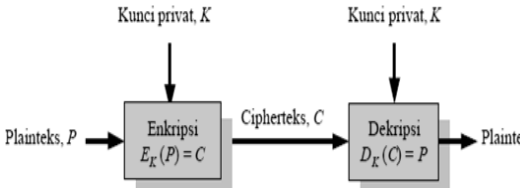
Secara etimologi (ilmu asal usul kata), kata kriptografi berasal dari gabungan dua kata dalam bahasa Yunani yaitu "*kriptos*" dan "*graphia*". Kata kriptos digunakan untuk mendeskripsikan sesuatu yang disembunyikan, rahasia atau misterius, sedangkan kata *graphia* berarti tulisan [3].

Dalam arti lain, *cryptography* adalah seni dan ilmu dalam mengamankan pesan. Dalam dunia kriptografi, pesan disebut *plaintext* atau *cleartext*. Proses untuk menyamarkan pesan dengan cara sedemikian rupa untuk menyembunyikan isi aslinya disebut enkripsi. Pesan yang telah dienkripsi disebut *ciphertext*. Proses pengembalian

sebuah *ciphertext* ke *plaintext* disebut dekripsi, namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan *data integrity*, *authentication* dan *non-repudiation Auto Complete Text* [3].

## 2.2 Kunci Simetris

Pada sistem kriptografi kunci simetri, kunci untuk enkripsi sama dengan kunci untuk deskripsi. Oleh karena itulah dinamakan kriptografi simetris. Sistem kriptografi kunci simetris mengasumsikan pengirim dan penerima pesan sudah berbagi kunci yang sama sebelum bertukar pesan. Keamanan sistem kriptografi simetris terletak pada kerahasiaan kuncinya. Ada puluhan algoritma kriptografi modern yang termasuk ke dalam sistem kriptografi simetris, diantaranya adalah DES (*Data Encryption Standard*), *Blowfish*, *Twofish*, *Triple*-DES, IDEA, *Serpent*, dan yang terbaru adalah AES (*Advanced Encryption Standard*). Untuk skema dari kunci simetris ditunjukan oleh Gambar 1 [3].

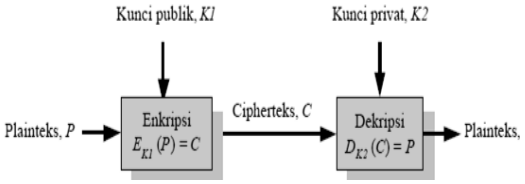



Gambar 1 Skema Kunci Simetris

## 2.3 Kunci Asimetris

Jika kunci untuk enkripsi tidak sama dengan kunci untuk deskripsi, maka kriptografinya dinamakan sistem kriptografi asimetri. Nama lainnya adalah kriptografi kunci publik (*public key cryptography*), sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun (diumumkan ke publik), sementara kunci untuk deskripsinya hanya diketahui oleh penerima pesan (karena itu rahasia).

Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim mengenkripsi pesan dengan menggunakan kunci publik. Hanya penerima pesan (*receiver*) yang dapat mendeskripsi pesan karena hanya ia yang mengetahui kunci privatnya sendiri. Contoh algoritma kriptografi kunci publik diantaranya RSA, *Elgamal*, DSA dan sebagainya. Gambar 2 menunjukkan skema kunci asimetris [3].




Gambar 2 Skema kunci asimetris

## 2.4 RC4 Stream Cipher

Algoritma RC4 (*Rivest Code*) *Stream Cipher* merupakan salah satu algoritma kunci simetris berbentuk *stream chipper* yang memproses unit atau *input* data, pesan ataupun informasi. Algoritma ini tidak harus menunggu sejumlah *input* data, pesan atau informasi tertentu sebelum diproses atau menambahkan *byte* tambahan untuk mengenkrip.

RC4 merupakan salah satu jenis *Stream Cipher*, yaitu memproses unit atau *input* data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan kadang-kadang bit (*byte* dalam hal RC4). Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah *input* data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip. Contoh *Stream Cipher* adalah RC4, Seal, A5, Oryx dan lain-lain. Tipe lainnya adalah *Block Cipher* yang memproses sekaligus sejumlah tertentu data (biasanya 64 bit atau 128 bit blok), contohnya *Blowfish*, DES, *Gost*, *Idea*, RC5, *Safer*, *Square*, *Twofish*, RC6, Loki97 dan lain-lain.

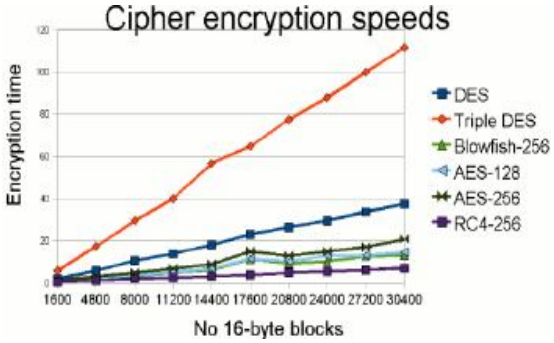
RC4 merupakan jenis aliran kode yang berarti operasi enkripsinya dilakukan per karakter 1 *byte* untuk sekali operasi. Algoritma kriptografi *Rivest Code* 4 (RC4) merupakan salah satu algoritma kunci simetris dibuat oleh RSA Data Security Inc (RSADSI) yang berbentuk *Stream Chipper*. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu : Rivest, Shamir, dan Adleman) [3]

## 2.5 Kecepatan RC4 Sebagai Salah Satu Metode Enkripsi

Kinerja RC4 sebagai metode enkripsi tergolong sangat cepat. Selain cepat, waktu RC4 tidak terpengaruh dengan panjang *keylength* yang dipakai. *Byte* K di-XOR-kan

dengan *plaintext* untuk menghasilkan *ciphertext* atau di-XOR-kan dengan *ciphertext* untuk menghasilkan *plaintext*. Enkripsi sangat cepat kurang lebih 10 kali lebih cepat dari DES [4].

Gambar 3 menunjukkan perbandingan waktu yang digunakan untuk enkripsi dari berbagai metode.




Gambar 3 Perbandingan waktu enkripsi dari berbagai metode

## 3. HASIL DAN PEMBAHASAN

Pada tahap ini merupakan tahap penerapan sistem pada keadaan yang sebenarnya agar dapat berfungsi sesuai kebutuhan, sehingga dapat diketahui apakah sistem yang dibuat sesuai dengan perancangan sebelumnya. Di sini akan dijelaskan bagaimana sistem ini memberikan contoh-contoh tampilan aplikasi yang terdapat pada Aplikasi sistem keamanan basis data dengan teknik kriptografi, menu dimana masing-masing menu memiliki fungsi tersendiri.

Spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam implementasi adalah sebagai berikut :

1. Perangkat lunak yang dibutuhkan (*required software*):
   a. Sistem Operasi yang digunakan adalah *Windows* 10*Pro* 64-*bit*.
   b. *NetBeans IDE* 8.0
   c. JDK (Java *Development* Kit) 8.
2. Perangkat keras yang dibutuhkan (*required hardware*):
   a. Lenovo G-40
   b. *Intel Celeron* 2.2 GHz
   c. HDD 320GB.
   d. *Monitor* 14 *inch* (1680x1050)
   e. *RAM* 2 GB DDR3

### 3.1 Pengujian Sistem

Pengujian merupakan tahap yang utama dalam pembuatan suatu aplikasi. Hasil pengujian yang didapat, akan dijadikan sebagai tolak ukur dalam proses pengembangan selanjutnya. Pengujian ini dilakukan untuk mengetahui hasil yang didapat dari aplikasi yang telah dibuat. Pengujian ini dilakukan untuk memeriksa hasil proses enkripsi *database* yang dilakukan oleh aplikasi, apakah sudah sesuai dengan yang diharapkan. Pengujian ini dilakukan dengan memasukkan sebuah sampel *database* yang akan kita proses enkripsi kedalam *form* aplikasi untuk keakuratan aplikasi.

### 3.2 Interface Aplikasi

a. Form Menu Login

Pada *form* ini *user* terlebih dahulu memasukan nama dan kata sandi sebelum masuk, pada *form* menu utama yang memiliki 4 menu yakni : Enkripsi, Dekripsi, Petunuk dan Tentang. Gambar 4 menunjukkan *form* menu Login.


Gambar 4 *Form* Menu Login

b. Form Menu Utama

Pada *form* ini *user* memilih menu yang akan dibuka sesuai kebutuhannya, terdapat 4 menu, yaitu: Enkripsi, Dekripsi, Petunjuk dan Tentang.

Pada menu Enkripsi berisikan *form* untuk memproses *database* yang ingin dienkripsi.

Pada menu Dekripsi berisikan *form* untuk memproses *database* yang telah dienkripsi dan akan dikembalikan dalam bentuk *database* asli.

Pada menu Petunjuk berisikan *form* tentang tata cara menggunkan aplikasi Ekripsi-Dekripsi *database* ini. Gambar 5 menunjukkan *form* menu Utama.


Gambar 5 *Form* menu Utama

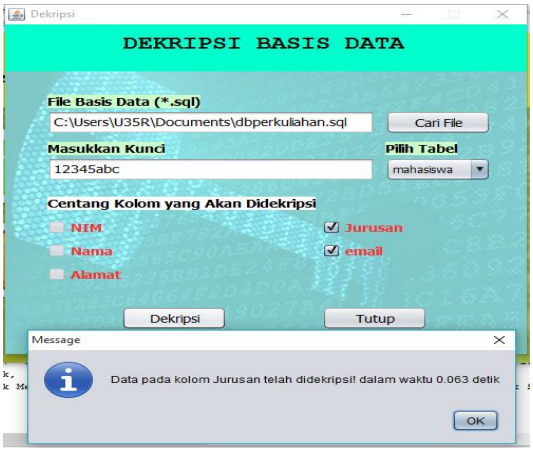
c. Form Menu Enkripsi

Pada *form* ini *user* meng-*input*-kan *database* yang isi data dalam tabelnya akan di enkripsi , setelah selesai meng*input*kan *file database* (*sql) dan memilih tabel mana yang akan di proses kemudian memasukan kunci dan tekan tombol Eknripsi untuk mmemproses. Gambar 6 menunjukkan *form* menu Enkripsi.


Gambar 6 *Form* menu Enkripsi

d. Form Menu Dekripsi

Pada form ini *user* memilih tombol cari *file* untuk mengimputkan *file database* yang telah terenkripsi sebelumnya, tombol pilih tabel untuk memilih tabel mana yang akan didekripsi, kemudian memasukan kunci yang dipakai pada proses enkripsi lalu centang kolom yang akan dienkripsi untuk memilih diantara dua kolom terakhir yang akan dienkripsi, tombol dekripsi untuk melakukan proses dekripsi, dan tombol tutup untuk keluar dari menu dekripsi. *Form* menu Dekripsi ditunjukkan oleh Gambar 7.




Gambar 7 *Form* menu Dekripsi

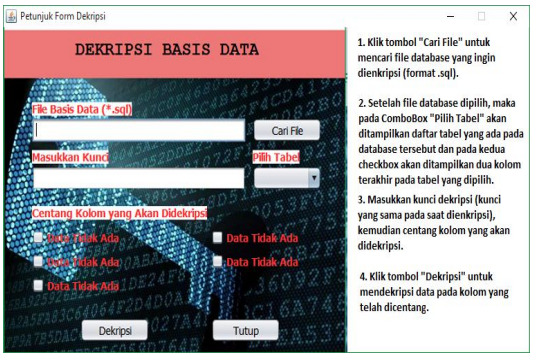
e. Form Menu Petunjuk

Pada *form* ini *user* memilih tombol enkripsi untuk melihat cara kerja tombol enkripsi begitupun dengan tombol yang lain untuk menjelaskan funsi-fungsi dari setiap menu utama. Gambar 8 menunjukkan *form* Petunjuk.


Gambar 8 *Form* menu Petunjuk

f. Form Menu Petunjuk Dekripsi

Pada form ini user memilih tombol form dekripsi dan akan tampil petunjuk pengunaan tombol dekripsi. Gambar 9 menunjukkan *form* menu Petunjuk Dekripsi..




Gambar 9 *Form* menu Petunjuk Dekripsi

## 4 KESIMPULAN

Dari penelitian dan pembahasan aplikasi enkripsi dengan metode RC (*Rivest Code 4* ) *Stream Cipher* maka dapat ditarik kesimpulan sebagai berikut :

1. Untuk proses kriptografi menggunkan metode RC4 (*Rivest Code*) *Stream Chipper*, hasil dari proses enkripsi dan deskripsi menunjukkan *file* yang telah dienkripsi (*Ciphertext*) kembali seperti *file* basis data aslinya (*plaintext*).
2. Algoritma RC4 *stream Cipher* dapat diimplementasikan untuk merubah *file* basis data asli dalam bentuk *file* basis data terenkripsi yang hasil akhirnya di konversi dalam bentuk *hexadecimal*.

## 5. SARAN

Saran yang perlu diperhatikan untuk penelitian lebih lanjut adalah:

1. Metode yang digunakan pada aplikasi Enkripsi ini dapat dikembangkan dengan metode yang lain. Kemudian bandingkan performanya antara metode Enkripsi ini dengan metode Enkripsi lainya
2. Perbaikan dalam proses enkripsi dapat lebih luas lagi yaitu pada bagian pilihan *field* (kolom) yang akan diproses untuk diterapkan dengan mengenkrip semua *field* (kolom) sesuai keinginan.
3. Untuk peneliatian selanjutnya *server database* dapat mengunakan *server database* selain xampp MySQL.
4. Untuk penelitian selanjutnya dapat menambahkan proses edit *database*-nya, agar fungsi aplikasinya lebih sempurna.

## DAFTAR PUSTAKA

[1] Haji, W.H. dan Mulyono, S., 2012, *Implementasi RC4 Stream Cipher Untuk Keamanan Basis Data*, Jurusan Sistem Informasi, Fakultas Ilmu Komputer, Universitas Mercu Buana, Jakarta Barat

[2] Suhendra, A., 2012, *Analisis Dan Implementasi Enkripsi Basis Data Dengan Algortima Kriptografi Blowfish*, Teknik Informatika, STMIK Amikom Yogyakarta.

[3] Munir, R., 2006, *Kriptografi*, Penerbit Informatika, Bandung

[4] Suryani, K.N., 2009, *Algoritma RC4 Sebagai Metode Enkripsi*, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika ITB, Bandung