KEAMANAN DATABASE DENGAN METODE RIVEST CODE 4 (RC4) DAN CAESAR CIPHER BERBASIS DESKTOP

Achmad Sri Muharyanto[1)], Titin Fatimah[2)]
[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : achmad.srim@gmail.com[1)], titin.fatimah@budiluhur.ac.id[2)]

Abstrak

Keamanan data merupakan aspek utama yang ada di dalam sistem operasi komputer yang kini telah menjadi suatu alat bantu utama dalam kehidupan manusia sehari-hari. Salah satunya pengguna database membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. PT. Anugerah Agung Abadi Logistics yang bergerak di bidang export-import dan logistics, yang memiliki database berupa data transaksi pengiriman. Sehingga data yang ada di dalam perusahaan harus dijaga semestinya agar tidak terjadi manipulasi data termasuk isi database. Salah satunya dengan pengamanan kriptografi dengan metode Algoritma RC4 dan Caesar Cipher agar isi record database yang disimpan menjadi lebih aman dan tidak ada yang dapat mengaksesnya. Penelitian ini menghasilkan keamanan database dengan metode Rivest Code (RC4) dan Caesar Cipher berbasis Desktop. Aplikasi pengamanan database menggunakan bahasa pemrograman Java. Aplikasi yang dibuat dapat memberikan keamanan lebih terhadap isi data yang bersifat rahasia ke dalam database tanpa takut adanya pihak lain yang dapat membaca isi dari datanya perusahaan.

Kata Kunci : Dekripsi, Enkripsi, Kriptografi, *RC* 4, *Caesar Cipher*, *Database*,

1. PENDAHULUAN

Teknologi komputer dan telekomunikasi saat ini telah mengalami kemajuan dan sudah menjadi suatu kebutuhan yang penting bagi setiap orang, karena banyaknya pekerjaan yang dapat diselesaikan dengan cepat. Salah satu dampak negatif di dalam perkembangan teknologi adalah adanya pencurian data, Salah satunya pengguna *database* membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. PT. Anugerah Agung Abadi Logistics yang bergerak di bidang *export-import* dan *logistics*, yang memiliki *database* berupa data transaksi pengiriman. Sehingga data pada perusahaan ini harus dijaga kerahasiaannya. Dengan adanya kriptografi menggunakan metode Algoritma RC4 dan Caesar Cipher maka isi dari *record database* yang disimpan agar terjaga lebih aman dan tidak ada yang dapat mengaksesnya. Pemilihan metode algoritma Kriptografi RC4 dan *Caesar Cipher* dikarenakan menyembunyikan dan menyamarkan pesan rahasia dalam suatu media penampung dan sistem penyandian. Algoritma RC4 (*Rivest Cipher* 4) juga salah satu algoritma kriptografi simetris yang paling populer dan bersifat *stream cipher[3]*. Dalam permasalahan yang diangkat dalam menyelesaikan masalah, yaitu pernah terjadi kecurangan manipulasi data oleh pihak yang tidak berwenang. Kecurangan tersebut sudah pernah terjadi 2 kali dalam bentuk *record database* yang berupa data transaksi pengiriman. Lalu untuk tujuannya adalah mengenkripsikan suatu *record* pada perusahaan tersebut agar keamanan *database* tidak dapat diakses dengan mudah oleh pihak yang tidak berhak menerima informasi tersebut, dengan menggunakan algoritma kriptografi RC4 dan Caesar Cipher[1][2]

2. METODE PENELITIAN

Penelitian ini dilaksanakan pada bulan Oktober sampai Desember 2017 di PT. Anugerah Agung Abadi Logistics, Kec.Tanjung Priok–Jakarta Utara. Jenis penelitian yang dikembangkan menggunakan RAD (*Rapid Application Development*), model ini dibuat oleh James Martin untuk membuat sistem yang cepat tanpa harus mengorbankan kualitas, yaitu suatu desain/fase penelitian untuk mempelajari perencanaan, perancangan, dan kontruksi dengan cara pendekatan, atau pengumpulan data sekaligus.

2.1. Perancangan Sistem

Perancangan menggunakan *Entity Relationship Diagram* dan *Flowchart* untuk menggambarkan sebuah proses yang dapat dilakukan oleh user dan alur aplikasi yang dibuat.

2.2. Perancangan Database

Menggambarkan entitas antar relasi di dalam sistem tersebut yang akan dijadikan database menggunakan *Entity Relationship Diagram.*

2.3. Perancangan Interface (antarmuka)

Perancangan antarmuka (*user interface*)

meliputi struktur menu, input, dan output pada halaman-halaman untuk bagian user agar nyaman saat digunakan.

2.4. Implementasi

Sistem ini diimplementasikan dengan bahasa pemrograman Java yang berbasis Dekstop. Penggunaan metode dengan menggunakan RC4 dan Caesar Cipher agar saat mengamankan data lebih aman dan MySQL sebagai tempat penampung basisdata yang digunakan untuk mengamankan atau mengenkripsikan data yang tersimpan.

2.5. Pengujian

Tahap pengujian terdiri dari dua macam:

a. Pengujian enkripsi record database.
b. Pengujian dekripsi record database.

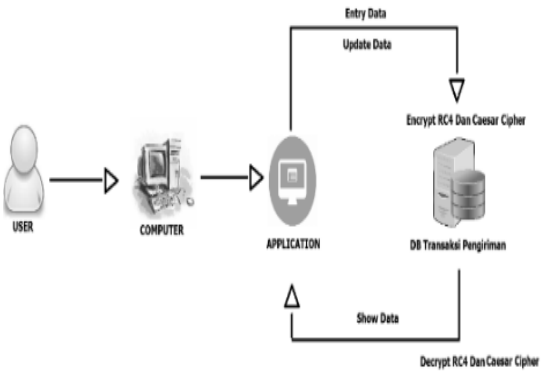
3. HASIL DAN PEMBAHASAN

3.1. Analisa Masalah

Kemajuan teknologi telah banyak orang yang dapat mengakses segala bentuk dari data dengan sangat mudah, termasuk halnya yang bersifat rahasia. Hal ini dapat menimbulkan masalah, terutama pada pengamanan data yang akan masuk ke dalam *database* yaitu data transaksi pengiriman pada suatu perusahaan yang sebagian data dan informasinya merupakan rahasia dan aset perusahaan.

3.2. Arsitektur Sistem

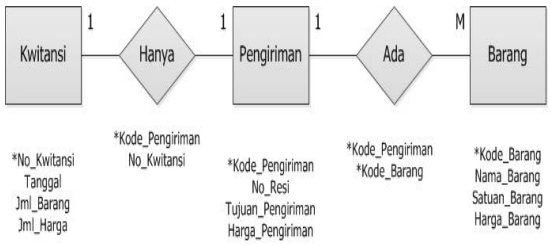
Berikut ini merupakan arsitektur sistem, untuk dapat memahami konsep aplikasi yang dibangun. Pada arsitektur sistem menggambarkan proses dari keseluruhan sistem yang dibuat.



Gambar 1 : ***Arsitektur Sistem***

3.3. ERD (*Entity Relationship Diagram*)

Entity Relationship Diagram (ERD) telah berisi sekumpulan isi dari entitas dan isi dari relasi. Masing-masing telah dilengkapi dengan atributnya yang mewakili seluruh data yang ada.

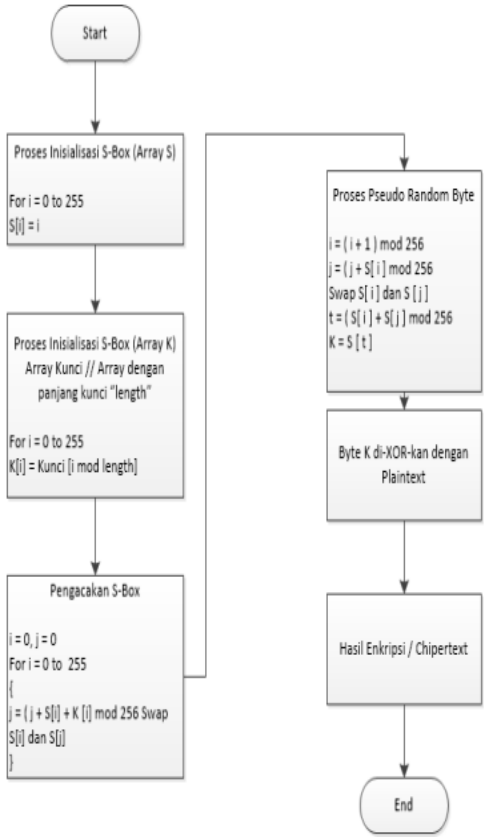


Gambar 2 : ***ERD (Entity Relationship Diagram)***

3.4. Flowchart

a. *Flowchart* Proses Enkripsi RC4

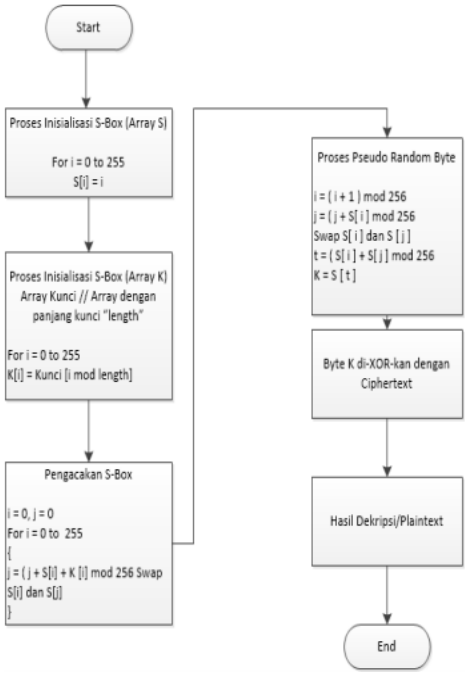
Flowchart ini menjelaskan alur proses enkripsi RC4. Alurnya seperti berikut :



Gambar 3 : ***Flowchart Enkripsi RC4***

b. *Flowchart* Proses Dekripsi RC4

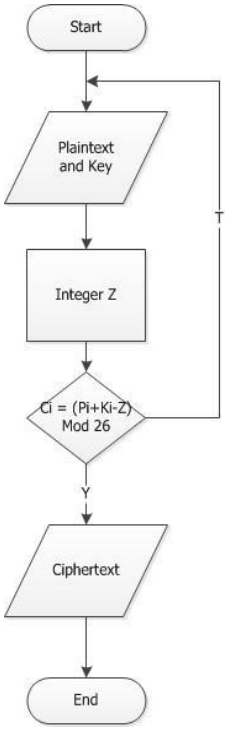
Flowchart ini menjelaskan alur proses dekripsi RC4. Alurnya seperti berikut:



Gambar 4 : ***Flowchart Dekripsi RC4***

c. *Flowchart* Proses Enkripsi Caesar Cipher

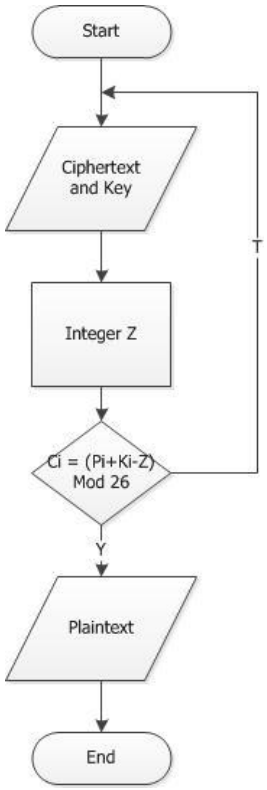
Flowchart ini menjelaskan alur proses enkrpsi Caesar Cipher. Alurnya seperti berikut :



Gambar 5 : ***Flowchart Enkripsi Caesar Cipher***

d. *Flowchart* Proses Dekripsi Caesar Cipher

Flowchart ini menjelaskan alur proses dekripsi Caesar Cipher. Alurnya seperti berikut:



Gambar 6 : ***Flowchart Dekripsi Caesar Cipher***

3.5. Tampilan Layar

Dalam tampilan layar akan diuraikan mengenai tampilan layar aplikasi, mulai dari dijalankan sampai akhir progres. Berikut akan dikasih penjelasan dan gambar mengenai tampilan yang ada di aplikasi ini.

a. Tampilan Layar Menu Login

Tampilan layar dari Menu *Login* muncul pada saat aplikasi ini pertama kali dijalankan. Di dalam Menu *Login* terdapat *Username* dan *Password*. Pengguna harus memasukan *username* dan *password* yang sesuai agar dapat masuk ke aplikasi dekstop kriptografi.

Gambar 7 : ***Tampilan Layar Menu Login***

b. Tampilan Layar Menu Lupa Password

Tampilan layar menu Lupa Password dapat muncul pada saat user mengklik lupa password. Menu ini digunakan untuk membantu user mengetauhi passwordnya kembali.

Gambar 8 : ***Tampilan Layar Menu Lupa Password***

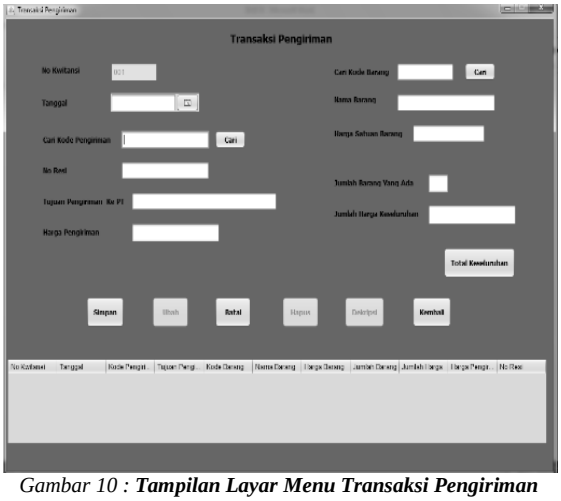
c. Tampilan Layar Menu Utama

Pada Menu Utama terdapat menu yang dapat dipilih, diantaranya Menu Master Pengiriman, Master Barang, Transaksi Pengiriman, *Help*, Ganti Password, *About*.

Gambar 9 : ***Tampilan Layar Menu Utama***

d. Tampilan Layar Menu Transaksi Pengiriman

Tampilan ini akan muncul ketika *user* memilih Menu Transaksi Pengiriman. Maka tampilan layar menu transaksi pengiriman.

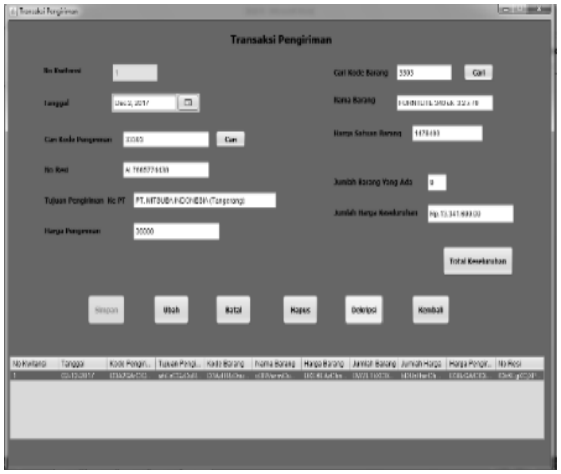


Gambar 10 : ***Tampilan Layar Menu Transaksi Pengiriman***

Jika *user* ingin menambah data transaksi pengiriman, *user* harus mengisi setiap *field* yang ada lalu memilih tombol simpan. Ketika *user* memilih tombol simpan, maka data tersebut telah terenkripsi dan tersimpan di dalam database transaksi pengiriman.

Gambar 11 : ***Tampilan Layar Pada Tabel Sesudah Data Disimpan Dan Dienkripsi***

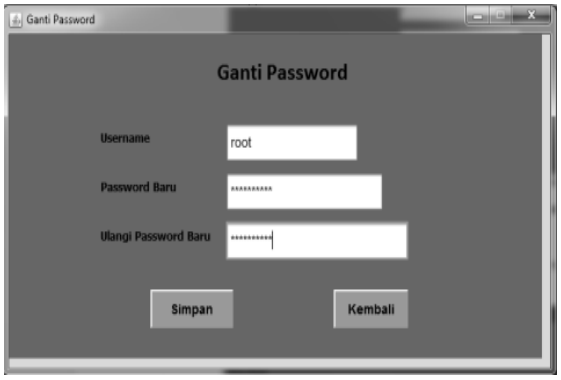
Setelah data berhasil ditampilkan ke dalam tabel, selanjutnya dapat memilih tombol dekripsi. Jika *user* memilih tombol dekripsi maka data yang ada di dalam *field* akan terdekripsi.



Gambar 12 : ***Tampilan Layar Menampilkan Data Yang Terdekripsi Pada Field***

e. Tampilan Layar Menu Ganti *Password*

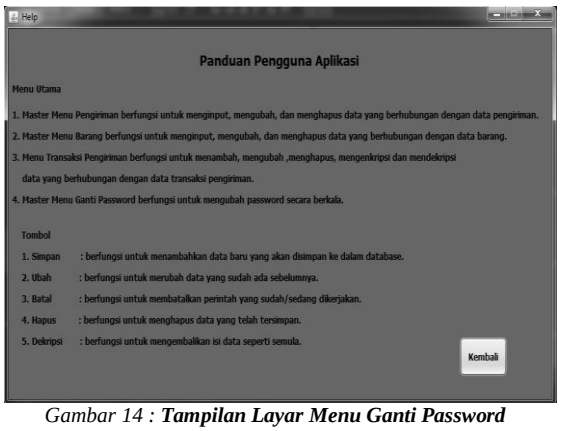
Tampilan ini akan muncul ketika *user* memilih Menu Ganti *Password*.



Gambar 13 : ***Tampilan Layar Menu Ganti Password***

f. Tampilan Layar Menu Help

Tampilan ini akan muncul ketika *user* memilih Menu Help.



Gambar 14 : ***Tampilan Layar Menu Ganti Password***

3.5. Pengujian dan Analisis

Setelah semuanya terpenuhi baik aplikasi yang dibuat, maka selanjutnya adalah menguji coba aplikasi yang telah dibuat dan dapat diuraikan mengenai pengujian enkripsi maupun dekripsi pada record *database*. Pengujian tersebut nantinya akan mendapatkan hasil perbandingan data setelah dan sebelum enkripsi.

Tabel 1 : Hasil Pengujian

Data	Karakter Asli	Jumlah Karakter (Byte)	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi (Byte)	Waktu Eksekusi Enkripsi (Mil/detik)
Cari Kode Pengiriman	22202	5	DHM1GAnClQLCjykxCcO6KVLDqQB6	28	0.023
No. Resi	AL9934222345	12	fQk8FwrCgnzDn2UnBMOiaH3DoRA0NMOWw5DDo8OBw55l	44	0.039
Harga Pengiriman	29000	5	DHozGA/ClQLCjykxCcO6KVLDqQB6	28	0.023
Cari Kode Barang	7707	4	A3wzERzDvizCk3ArE8K7LFvDrQc=	28	0.023
Harga Satuan Barang	664778	6	AH83EQbCjmnCoTVoE8OgaFfDoAR9YA==	32	0.031
Jumlah Harga Keseluruhan	Rp.13.324.560,00	10	bDUxHwrChH/Dn2cgC8OjexnCt1o0RcKTw4jCp8KWwpdqPBvCicOk	52	0.047
Rata-Rata		42/6 = 7	-	212/6= 35	0,028

3.6. Evaluasi Program

Evaluasi program adalah tahap akhir yang perlu dilakukan dalam membangun suatu aplikasi yang dibuat, yang tujuannya mengetahui hasil yang dicapai dari aplikasi yang dibuat. Berdasarkan uji coba program yang dilaksanakan maka akan diketahui kurang lebihnya pada apa yang dibuat, berikut hasil evaluasi yang diperoleh:

a. Kelebihan

1) *User* tidak perlu menginput *key* lagi ketika ingin mengenkripsi data.
2) Data yang diinput akan terjamin keamananya karena sudah melalui proses enkripsi.
3) Karena tampilannya yang sederhana, agar memudahkan *user* di dalam penggunaan aplikasi tersebut.

b. Kekurangan

1) Tidak bisa diakses dimana saja karena tidak berbasis *website*.
2) *Key* yang digunakan untuk enkripsi dan dekripsi bersifat dinamis.
3) *Enkripsi* hanya bisa per *record.*

4. KESIMPULAN

Berdasarkan analisa yang dilakukan terhadap permasalahan dan aplikasi yang dikembangkan, maka adanya kesimpulan yaitu:

a. Enkripsi RC4 *Stream Cipher* dan *Caesar Cipher* ini dapat diimplementasikan pada aplikasi keamanan *database*.
b. Pada aplikasi yang dibuat dapat mengamankan isi *record* yang akan masuk ke dalam database dengan pengamanan menggunakan metode *Rivest Code* 4 (RC4) dan *Caesar Cipher* sehingga data yang disimpan di dalam *database* akan susah untuk diretas.
c. Pada aplikasi tersebut dapat dijalankan sesuai dengan spesifikasi yang telah dirancang sebelumnya.

DAFTAR PUSTAKA

[1] Agung, H and Budiman (2015) Implementasi Affine Chiper Dan RC4 Pada Enkripsi File Tunggal. Jakarta: Prosiding *SNATIF*.

[2] Priyono (2016) 'Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks', ISSN : 2407-389X, 3, Nomor:, pp. 351–356.

[3] Widarma, A (2016) 'Kombinasi Algoritma AES, RC4 Dan Elgamal Dalam Skema Hybrid Untuk Keamanan Data', CESS Journal Of Computer Engineering System And Science. 1(1), pp. 11–19.