APLIKASI KRIPTOGRAFI UNTUK KEAMANAN DATABSE DENGAN METODE RC4 DAN ELGAMAL BERBASIS WEB PADA JXL DESIGN CO

Gilang Ammary[1)], Sri Mulyati[2)]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : gilangammary77@gmail.com[1)], sri.mulyati@budiluhur.ac.id[2)]

Abstrak

Keamanan dan kerahasiaan data merupakan hal yang penting dalam system operasi computer, salah satunya pada database. Data yang bersifat rahasia perlu dibuatkan penyimpanan dengan keamanan agar tidak terjadi kebocoran informasi dan pencurian data oleh pihak yang tidak bertanggung jawab. JXL Design Co adalah salah satu perusahan swasta yang bergerak dalam bidang penyedia jasa dan produk desain grafis. Semua data-data pada JXL Design Co di simpan ke dalam database, seperti data pelanggan dan data transaksi. Oleh karena itu dibutuhkan suatu aplikasi yang dapat mempermudah pengguna dalam menyimpan sekaligus untuk mengamankan data tersebut dengan aman agar tetap terjaga kerahasiaannya. Pengamanan data ini dilakukan dengan teknik kriptografi dengan metode algoritma Rivest Code 4 (RC4) dan Elgamal. Algoritma Rivest Code 4 (RC4) di pilih karena kecepatan prosesnya dan kesederhanaannya dalam menangani banyak aplikasi, sehingga mudah untuk mengembangkan implementasi yang efisien pada software dan juga hardware dan algoritma Elgamal karena keamanan Elgamal terletak pada sulitnya menghitung logaritma diskrit. Logaritma ini disebut logaritma diskrit karena nilainya berhingga dan bergantung pada bilangan prima yang digunakan. Pada penelitian ini penulis berusaha membuat aplikasi pengamanan database dengan kriptografi Rivest Code 4 (RC4) dan Elgamal. Aplikasi kriptografi ini berbasis web dengan menggunakan bahasa pemrograman Java. Dengan adanya aplikasi ini, penulis berharap pengguna dapat menyimpan data ke dalam database dengan aman.

Kata kunci: Algoritma, *Rivest Code 4* (RC4), Elgamal, Kriptografi, *Database.*

1. PENDAHULUAN

Penerapan dari teknologi komputer di Indonesia sudah menjadi kebutuhan penting dalam membantu kelancaran pada setiap kegiatan dari segi pendidikan sampai segi ekonomi. Berbagai data atau informasi sudah semakin mudah dilakukan dengan adanya komputerisasi yang bisa dilakukan tanpa adanya media fisik. Namun terkadang keamanan pertukaran data ini masih kurang diperhatikan, dampak negatif dari kelemahan keamanan ini adalah adanya pencurian data. Dengan adanya pencurian maka keamanan dalam pertukaran dan penyimpanan data merupakan hal penting karena untuk mengurangi tindak kriminal yang bisa terjadi apabila terjadi pencurian data.

JXL Design Co adalah salah satu perusahan swasta yang bergerak dalam bidang penyedia jasa dan produk desain grafis. Data perusahaan ini harus dijaga kerahasiaannya agar tidak terjadi pencurian data termasuk database, seperti data transaksi. Salah satunya dengan pengamanan kriptogra dengan metode algoritma RC4 dan Elgamal agar *record database* yang disimpan menjadi aman dan tidak dapat di akses dengan mudah.

Pada penelitian ini dirancang dengan sebuah sistem aplikasi berbasis web dengan algoritma kriptografi RC4 *(Rivest Code 4)* dan metode Elgamal. Pemilihan metode algoritma kriptografi RC4 karena algoritma ini memiliki mekanisme yang cukup sederhana dan mudah di mengerti dalam menyamarkan dan menyembunyikan pesan rahasia pada suatu media penyimpanan dan sistem penyandian. Dan pemilihan algoritma Elgamal digunakan untuk mengamankan kunci dari algoritma RC4.

Dengan melihat latar belakang diatas maka dapat diambil dengan beberapa pokok permasalahan yang dimiliki oleh JXL DESIGN CO, bagaimana cara mengamankan isi dari *database* yang bersifat rahasia agar tetap terjaga keaslian dan kerahasiaannya. Dibuatnya aplikasi pengamanan database ini untuk mengamankan isi dari database pada JXL Design Co agar tidak terjadi kebocoran informasi dan pencurian data oleh pihak yang tidak berwenang.

Adapun tujuan penulisan dari jurnal ini adalah sebagai berikut :

a. Mengamankan isi dari *database* pada JXL Design Co agar tidak dapat diketahui dan dimodifikasi oleh pihak yang tidak berwenang.
b. Dapat mengimplementasikan metode algoritma kriptografi RC4 dan Elgamal dalam bentuk aplikasi berbasis *web*.

2. METODE PENELITIAN

2.1 Algoritma RC4 *(Rivest Code 4)*

Algoritma RC4 *(Rivest code 4)* ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol

keamanan RSA, digunakan secara luas pada beberapa aplikasi dan umumnya dinyatakan sangat aman. Algoritma RC4 merupakan metode penyandian pesan teks yang melakukan enkripsi per *bit* sehingga kelebihan dari metode ini kerusakan pada satu *bit* tidak mempengaruhi keseluruhan isi pesan.

Pada RC4 dihasilkan *pseudo random stream bit*. Seperti halnya stream cipher lainnya, algoritma RC4 ini dapat digunakan untuk mengenkripsi dengan mengkombinasikannya dengan plainteks menggunakan *Exclusive-or* (Xor). Untuk proses dekripsi dilakukan cara yang sama dan dengan kunci yang sama, karena Xor merupakan fungsi simetrik. Secara garis besar proses algoritma RC4 dibagi menjadi dua bagian yaitu, KSA *(Key Scheduling Algorithm)* dan PRGA *(Pseudo Random Generation Algorithm)* [2].

a. Algoritma Proses Enkripsi RC4

Proses enkripsi algoritma RC4 secara garis besar terbagi menjadi dua bagian, yaitu : *key setup* atau *key scheduling algorithm* (KSA) dan *stream generation* atau *pseudorandom generation algorithm* (PGRA) dan proses XOR dengan stream data. Berikut penjelasan algoritma RC4 *stream cipher* :

Pada proses *key setup/key scheduling algorithm* (KSA) terdapat tiga tahapan pada bagian ini:

1) Inisialisasi S-Box
2) Menyimpan kunci dalam *key byte array*
3) Membandingkan sebuah nilai yang akan di jadikan aturan untuk permutasi S-Box

Kemudian pada pada proses *stream generation* atau *pseudorandom generation algorithm* (PGRA) akan dikenakan operasi XOR untuk menghasilkan *ciphertext* atau sebaliknya. Untuk lebih jelasnya perhatikan algoritma berikut:

1) Isi i dan j dengan nilai 0
2) Untuk i=0 hingga i=panjang *plaintext*
3) Isi nilai i dengan hasil operasi (i+1) mod 256
4) Isi nilai j dengan hasil operasi (j+S(i)) mod 256
5) Tukar nilai S(i) dan S(j)
6) Isi nilai t dengan hasil operasi (S(i)+S(j)) mod 256
7) Isi nilai y dengan nilai S(t)
8) Nilai y dikenakan operasi XOR *plaintext*
9) Tambahkan i dengan 1, kembali ke 2

b. Algoritma Proses Dekripsi RC4

Pada dasarnya proses algoritma dekrispsi RC4 sama mirip dengan proses enkripsi RC4, namun perbedaanya adalah hanya pada saat stream generation, yang mana akan menghasilkan plainteks semula. Maka cipherteksnya akan di-XOR kan terhadap pseudorandom bytenya. Algoritma key setup sama dengan proses enkripsi yang di proses inisialisasi S-Box, penyimpanan kunci ke dalam kunci byte array hingga proses insialisasi S-Box berdasarkan kunci stream yang sama. Perbedaanya hanya pada stream generationya, yaitu yang dioperasikan bersama kunci stream adalah *ciphertext* untuk menghasilkan plainteks [2]. Berikut algoritma proses dekripsi RC4 :

1) Indeks i dan j di isi dengan nilai 0
2) Untuk i=0 hingga i=panjang ciphertext (panjang ciphertext=plaintext)
3) Nilai i di isi dengan hasil operasi (i+1) mod 256
4) Nilai j di isi dengan hasil operasi (j+S(i)) mod 256
5) Tukar nilai S(i) dan S(j)
6) Isi nilai t dengan hasil operasi (S(i)+S(j) mod 256) mod 256
7) Nilai y di isi dengan nilai S(t)
8) Nilai y dikenakan operasi XOR terhadap *ciphertext*
9) Tambahkan i dengan 1, kembali ke 2

2.2. Algoritma Elgamal

Algoritma Elgamal ditemukan oleh ilmuwan Mesir, yaitu Taher Elgamal pada tahun 1985, merupakan algoritma kriptografi kunci publik. Proses algoritma elgamal terdiri menjadi tiga proses, yaitu proses pembentukan kunci, proses enkripsi, dan proses dekripsi [4].

Kriptografi elgamal pada awalnya digunakan untuk kebutuhan *digital signature*, namun kemudian dimodifikasi sehingga dapat digunakan untuk pengamanan seperti enkripsi dan deskripsi. Kriptografi Elgamal digunakan kedalam perangkat lunak *security* yang dikembangkan oleh GNU, program PGP, dan pada sistem *security* lainnya.

Kriptografi elgamal tidak dipatenkan oleh pembuatnya melainkan didasarkan atau penyempurnaan dari pada kriptografi Diffei-Hellman, yaitu sebuah kriptografi kunci publik yang dikenalkan oleh Whitfield Diffie dan Martin Hellman. Sehingga hak paten kriptografi Diffie-Hellman mencakup kriptografi Elgamal. Dan hak paten ini telah berakhir pada tahun 1997 dan mulai pada saat itu kriptografi Elgamal dapat di komersilkan secara umum [3].

a. Algoritma *Generate Key*

Algoritma Elgamal merupakan sepasang kunci yang dibangkitkan dengan memilih bilangan prima p dan dua buah bilangan acak (random) g dan x, dengan syarat bahwa nilai g dan x lebih kecil dari p yang memenuhi persamaan 1 [1].

$$Y = (g \hat{} x) \bmod p \quad \text{Persamaan (1)}$$

b. Algoritma Proses Enkripsi Elgamal

Proses enkripsi adalah proses mengubah *plaintext* menjadi *ciphertext*. Pada proses ini

digunakan kunci *public* yaitu p,g,y. Proses algoritma elgamal dalam mengenkripsi pesan terdapat pada persamaan 2 dan 3 [1].

a = (g ^ k) mod p	Persamaan (2)
b = (y ^ k.m) mod p	Persamaan (3)

c. Algoritma Proses Dekripsi Elgamal

Merupakan proses mengubah pesan rahasia (*ciphertext*) menjadi pesan asli (*plaintext*). Proses dekripsi menggunakan kunci pribadi *x* dan *p* untuk mendekripsi *a* dan *b* menjadi *plaintext* (m) dengan persamaan 4 [1].

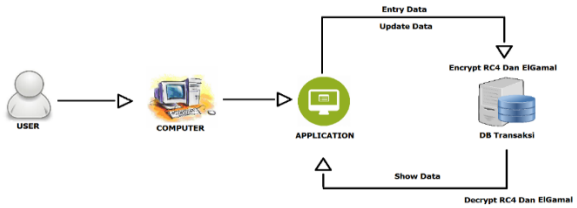
m = b . a^(p-1-x) mod p	Persamaan (4)

1) Penentuan nilai Gamma dan Delta. Nilai Gamma(a) diperoleh dari *ciphertext* dengan urutan ganjil, sedangkan Delta(b) diperoleh dari urutan genap.
2) Hitung *plaintext* m dengan persamaan rumus tersebut.
3) Ubah nilai m yang didapat ke dalam nilai ASCII
4) Susun *plaintext* dengan urutan m1,m2,…,mN.

3. HASIL DAN PEMBAHASAN

3.1. Arsitektur Sistem

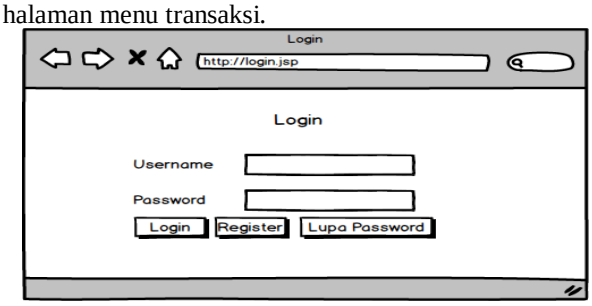
Arsitektur sistem merupakan struktur sebuah system, arsitektur system berkaitan erat dengan aplikasi yang dibuat, seperti perangkat keras, perangkat lunak, maupun lingkungan pendukungnya. Arsitektur system secara garis besaar menggambarkan proses dari keseluruhan system. Untuk lebih memahaiminya perhatikan gambar Arsitektur Sistem di bawah ini.



Gambar 1 : ***Arsitektur Sistem***

3.2. Rancangan Layar *Form Login*

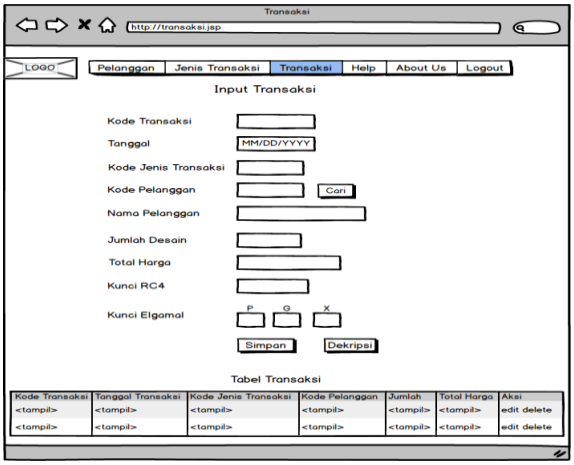
Pada menu ini pengguna harus memasukkan *username* dan *password* yang sudah dimiliki terlebih dahulu pada form yang telah disediakan. Setelah *login* berhasil, pengguna akan diarahkan menuju halaman menu transaksi.



Gambar 2. ***Rancangan Layar Form Login***

3.3. Rancangan Layar Menu Transaksi

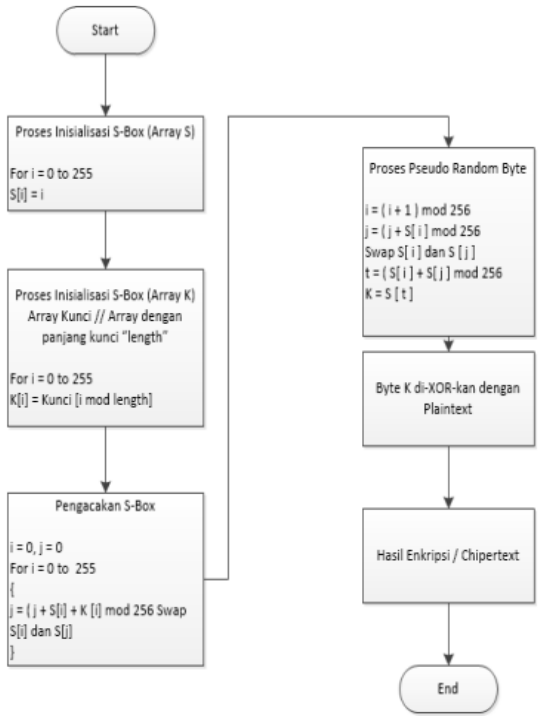
Rancangan layar menu transaksi berfungsi untuk menginput data transaksi. Pada menu transaksi terdapat 2 *button* dan *link* aksi yaitu simpan, dekripsi. *Button* simpan berfungsi untuk menyimpan data transaksi kedalam *database*. *Aksi edit* berfungsi untuk mengubah data transaksi yang sudah disimpan didalam table jenis transaksi pada *database*. *Aksi* delete berfungsi untuk menghapus data jenis transaksi dari table transaksi di *database*, dan *button* dekripsi untuk melakukan proses pengubahan isi data seperti semula.



Gambar 3. ***Rancangan Layar Menu Transaksi***

3.4. *Flowchart* Enkripsi RC4

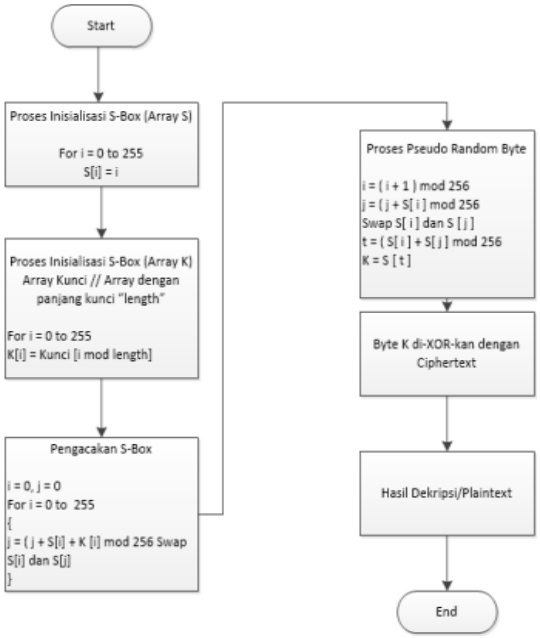
Pada *flowchart* enkripsi RC4 menjelaskan alur proses enkripsi pada algoritma RC4, yaitu mengubah *plaintext* menjadi *ciphertext.*



Gambar 4. ***Flowchart Enkripsi RC4***

3.5. *Flowchart* Dekripsi RC4

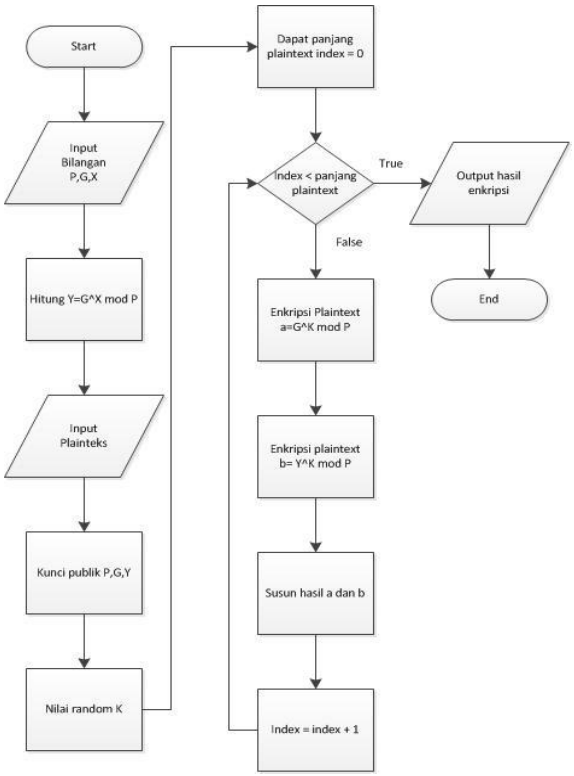
Pada *flowchart* dekripsi RC4 menjelaskan alur proses dekripsi pada algoritma RC4, yaitu mengembalikan *ciphertextt* menjadi *plaintext.*



Gambar 5. ***Flowchart Dekripsi RC4***

3.6. *Flowchart* Enkripsi Elgamal

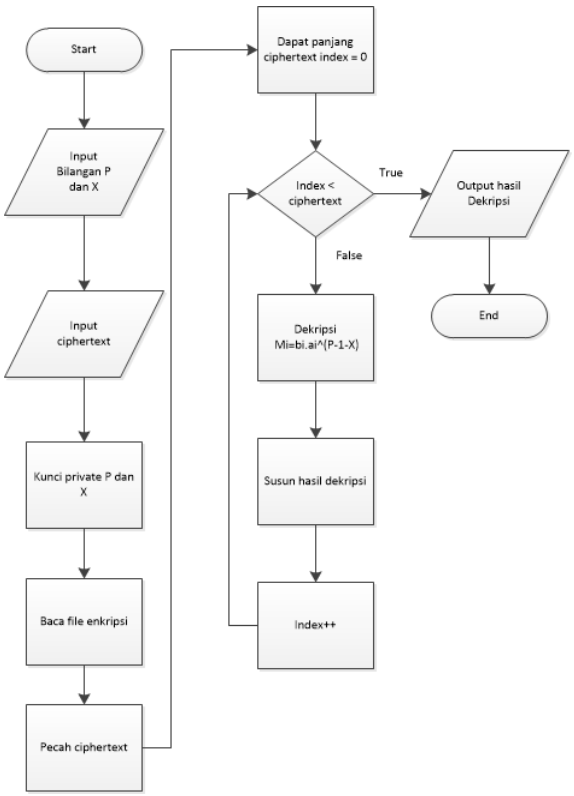
Flowchart enkripsi Elgamal menjelaskan tentang alur proses yang terjadi pada proses pengkodean *plaintext* ke *ciphertext*. Proses ini sangat penting dalam pembuatan aplikasi ini



Gambar 6. ***Flowchart Enkripsi Elgamal***

3.7. Flowchart Dekripsi Elgamal

Flowchart dekripsi Elgamal menjelaskan tentang alur proses yang terjadi pada proses pengembalian *ciphertext* ke *plaintext*. Proses ini sangat penting dalam pembuatan aplikasi ini.



Gambar 7. ***Flowchart Dekirpsi Elgamal***

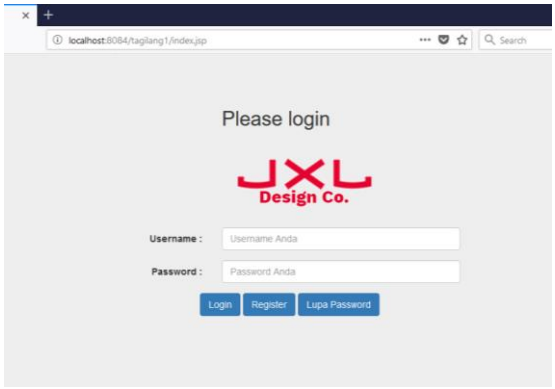
4. IMPLEMENTASI DAN UJI COBA PROGRAM

4.1. Tampilan Layar

Pada tampilan layar berisi menu dari aplikasi ini, mulai dari pertama kali aplikasi ini di jalankan sampai aplikasi selesai di jalankan. Berikut ini akan di berikan penjelasan tentang menu yang ada pada aplikasi ini:

a Tampilan Layar *Form Login*

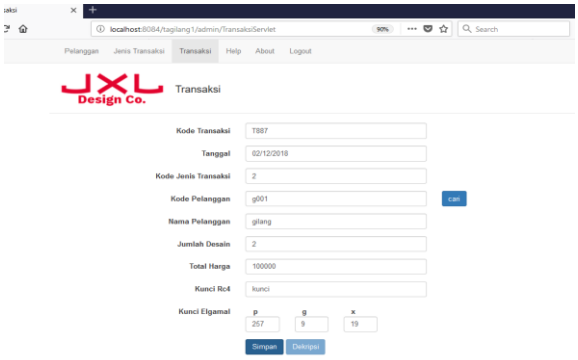
Form login pertama kali akan tampil ketika aplikasi dijalankan. Untuk masuk ke menu transaksi pengguna harus melakukan *login* terlebih dahulu.



Gambar 8. ***Tampilan Layar Form Login***

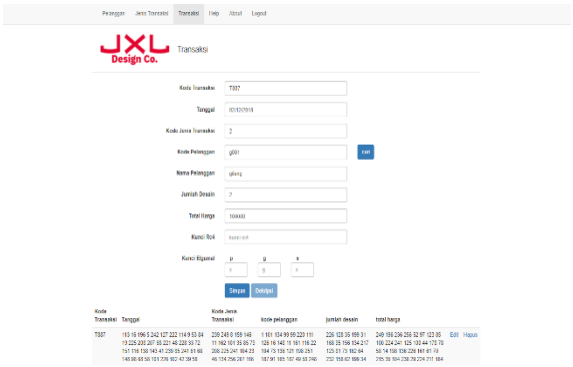
b. Tampilan Layar *Form* Transaksi

Menu ini akan tampil jika pengguna memilih Menu Transaksi, pada menu ini pengguna bisa menginput data dengan mengisi *form* transaksi terlebih dahulu dan memasukan kunci dari RC4 dan Elgamal, lalu pengguna memilih tombol "Simpan" untuk menyimpan data ke dalam *database.*



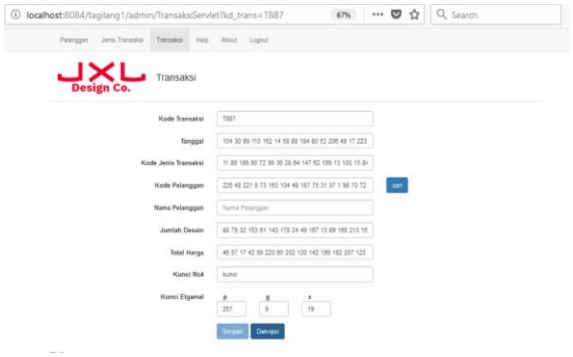
Gambar 9. ***Tampilan Layar Form Transaksi***

Setelah *record* berhasil tersimpan ke dalam *database*, *record* akan ditampilkan pada tabel di menu *form* transaksi, *record* yang ditampilkan pada tabel transaksi sudah terenkripsi.



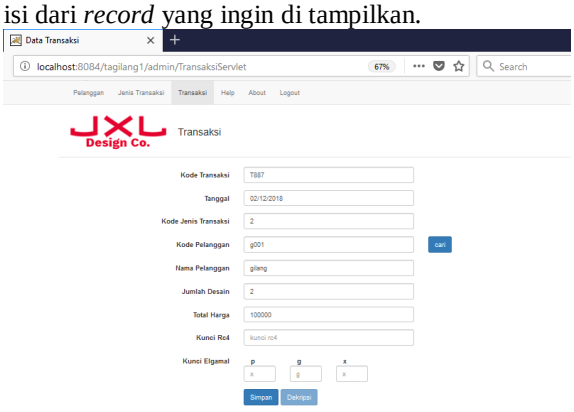
Gambar 10. ***Tampilan Record Yang Berhasil Tersimpan***

Jika pengguna ingin melihat isi dari *database*, maka pengguna harus memilih tombol "*Edit*" pada *record* yang ingin di lihat, lalu penguna harus mengisi kunci RC4 dan Elgamal yang sesuai dengan proses sebelum data di enkripsi.



Gambar 11. ***Tampilan Edit Transaksi***

Setelah pengguna memasukan kunci RC4 dan Elgamal lalu pilih tombol "Dekripsi" untuk melihat isi dari *record* yang ingin di tampilkan.



Gambar 12. ***Tampilan Proses Dekripsi Berhasil***

4.2. Evaluasi Program

Evaluasi program adalah tahap terakhir yang harus dilakukan dalam pengembangan suatu aplikasi, Evaluasi program bertujuan mengetahui hasil yang telah dicapai dari aplikasi yang dibuat. Berdasarkan hasil uji coba program dan eksekusi aplikasi yang dilakukan maka akan diketahui kelebihan dan kekurangan pada aplikasi yang dibuat, berikut adalah hasil evaluasi yang diperoleh:

a. Kelebihan

1) Terdapat autentikasi *Username* dan *Password* pada *Form Login*.
2) Program yang *user friendly*, karena memilik tampilan yang sederhana dan jelas, serta memiliki panduan penggunaan di dalam aplikasi tersebut.
3) Keamanan *database* yang telah dienkripsi sangat tinggi karena menggunakan 2 metode kriptografi, yaitu RC4 *(Rivest Code 4)* dan Elgamal.

b. Kekurangan

1) Aplikasi hanya dapat digunakan pada database yang sudah ditentukan oleh *user*.
2) Aplikasi ini hanya dapat mengenkripsi dan dekripsi *database* per *record* dalam satu kali proses.
3) Hasil *text* asli ke enkripsi bertambah panjang.

5. KESIMPULAN

Berdasarkan pada hasil Analisa dan pengujian yang telah di lakukan terhadap pokok permasalahan dan aplikasi yang telah kami kembangkan, maka didapatkan suatu kesimpulan, sebagai berikut:

a. Enkripsi RC4 *(Rivest Code 4)* dan Elgamal ini dapat diimplementasikan pada aplikasi keamanan *database* menggunakan bahasa pemrograman Java Web dan *database* MySQL.
b. Aplikasi kriptografi ini dapat mengamankan *record* data yang masuk ke dalam *database* dengan teknik kriptografi menggunakan metode RC4 *(Rivest Code 4)* dan Elgamal sehingga data yang tersimpan sulit untuk dibaca.
c. Aplikasi ini dapat di jalankan sesuai spesifikasi teknis yang telah dirancang.

DAFTAR PUSTAKA

[1] Adhar, D. (2014). PENGAMANAN SQLITE DATABASE MENGGUNAKAN KRIPTOGRAFI ELGAMAL. Seminar Nasional Informatika 2014.

[2] Harsa, A. K. (2014). Keamanan Data Dengan Menggunakan Algoritma Rivest Code 4 (Rc4) Dan Steganografi Pada Citra Digital. INFORMATIKA Mulawarman. Februari, 9(1).

[3] Triase. (2015). KRIPTOGRAFI ELGAMAL MENGGUNAKAN METODE MERSENNE. Jurnal ilmiah "INTEGRITAS" Vol.1 No.4.

[4] Rochmat, N., Isnanto, R. R., & Somantri, M. (2012). Implementasi Algoritma Kriptografi Elgamal Untuk Keamanan Pesan (Message Security). Jurnal VOL. 1, No.3, pp. 82-88.