IMPLEMENTASI KRIPTOGRAFI DENGAN METODE ALGORITMA ELGAMAL UNTUK KEAMANAN DATABASE BERBASIS JAVA DESKTOP PADA PT. MAKMUR SUPRA NUSANTARA

Gama Anugrah Sahputra[1)], **Titin Fatimah**[2)]
[1,2]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 : gamasahputra@gmail.com[1)], titin.fatimah@budiluhur.ac.id[2)]

ABSTRAK

PT. Makmur Supra Nusantara adalah perusahaan yang bergerak di bidang perdagangan produk kebutuhan bahan bangunan (semen), yang mempunyai customer dari berbagai daerah di Jabodetabek. Perusahaan ini memiliki beberapa data-data penting yang perlu dijaga kerahasiaannya. Dengan perkembangan teknologi dan informasi yang semakin pesat menyebabkan proses pengiriman data dapat dilakukan dengan mudah melalui berbagai macam media, tentunya dibutuhkan keamanan dalam penyimpanan data dan kerahasiaan data tersebut. Salah satu cara yang digunakan yaitu dengan mengenkripsi data tersebut melalui aplikasi kriptografi, untuk menangani permasalahan yang ada pada PT. Makmur Supra Nusantara maka diperlukan aplikasi pengamanan data yang dapat mengamankan database yang dimiliki. Aplikasi ini dapat mengamankan dan menjaga kerahasiaan data dan informasi PT. Makmur Supra Nusantara dari terjadinya pencurian dan manipulasi data oleh pihak yang tidak bertanggung jawab. Setelah proses enkripsi sudah dilakukan akan mengeluarkan output yang tentunya tidak dapat dibaca atau tidak bisa digunakan oleh pihak yang tidak bertanggung jawab. Bahasa pemograman yang digunakan pada aplikasi ini adalah Java NetBeans IDE 8.2 dengan metode Algoritma Elgamal. Karena algoritma Elgamal termasuk algoritma asimetris maka untuk proses kriptografi dibutuhkan dua kunci yaitu kunci publik untuk proses enkripsi dan kunci private untuk proses dekripsi. Dengan menggunakan aplikasi ini, PT. Makmur Supra Nusantara dapat menyimpan data transaksi yang bersifat rahasia ke dalam database tanpa takut ada orang lain yang mencuri atau membaca isi dari data transaksi tersebut.

Kata kunci: Kriptografi, Elgamal, Enkripsi, Dekripsi, Database

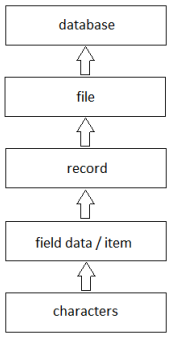
1. PENDAHULUAN

Semakin dengan berkembangnya teknologi komputer yang semakin maju dan tinggi, kemampuan mengakses dan menyediakan informasi data secara cepat perlu dilakukan di sebuah perusahaan. Adapun pentingnya data menyebabkan informasi data yang diinginkan hanya boleh diakses oleh orang-orang tertentu saja. PT. Makmur Supra Nusantara adalah perusahaan yang bergerak dalam bidang perdagangan produk kebutuhan bahan bangunan (semen). Di perusahaan tersebut terdapat data-data penting dari berbagai transaksi yang dilakukan oleh customer dari PT. Makmur Supra Nusantara. Perusahaan tersebut belum mempunyai aplikasi simpan dan keamanan data, atau masih menggunakan nota secara manual untuk melakukan transaksi pembayaran dan penyimpana data ke folder yang tidak diamankan keberadaannya. Aplikasi ini dibuat agar dapat menyimpan dan mengamankan informasi penting di dalam penyimpanan data di PT. Makmur Supra Nusantara dari pencurian data informasi oleh orang yang ingin mengambil data tersebut. Pada aplikasi ini data akan diinput ke dalam *database*, lalu untuk proses enkripsi dibutuhkan kunci publik yang sudah dibuat sebelumnya dan kunci private untuk proses dekripsi. Algoritma pada aplikasi ini yang digunakan untuk mengamankan data adalah algoritma Elgamal, informasi yang diamankan dalam sebuah database hanya berupa *plaintext* atau karakter yang dapat dibaca oleh orang perusahaan. Aplikasi ini hanya bisa mengenkripsi atau mendekripsi plaintext di *database* dengan cara per-*table*.

2. LANDASAN TEORI

2.1. Database

Database adalah suatu kumpulan dari data yang saling berkesinambungan satu dengan yang lainnya, yang disimpan secara bersama sedemikian rupa dan tanpa pengulangan yang tidak perlu, untuk memenuhi kebutuhan atau kumpulan file yang berhubungan, yang disimpan di media elektronis. *Database* merupakan bagian komponen yang penting, karena berfungsi sebagai penyedia informasi data oleh pemiliknya. Penerapan *database* dalam sistem disebut dengan *database system*[2].



Gambar 1 : Jenjang Data

2.2. Definisi Kriptografi

Kriptografi berasal dari bahasa yunani, *crypto* dan *graphia*. Kriptografi adalah teknik keamanan informasi data yang dilakukan dengan cara yaitu diolahnya informasi data awal atau (*plaintext*) dengan suatu kunci dan menggunakan metode enkripsi sehingga menjadikan suatu informasi baru atau (*ciphertext*) yang tidak bisa dibaca. *Ciphertext* tersebut dapat dikembalikan menjadi informasi data awal yang bisa dibaca (*plaintext*) melalui proses dekripsi pada sistem itu sendiri. Selain itu banyak metode yang ada di jenis kriptografi dan terbagi menjadi dua yaitu dengan algoritma Simetris dan Algoritma Asimetris[4].

2.3. Algoritma Kriptografi

Algoritma di dalam kriptografi adalah fungsi matematika yang digunakan untuk proses mengenkripsi dan proses mendekripsi. Konsep matematis yang didasari oleh algoritma adalah kekuatan pada relasi antara himpunan. Dengan sumber data yang dibutuhkan menunjukkan semakin kuat algoritma kriptografi tersebut maka akan semakin tidak bisa dipecahkan oleh pihak asing. Contohnya adalah mesin Enigma yang dikeluarkan oleh pemerintah Jerman pada masa perang dunia ke-2[3].

Gambar 2 : Mesin Enigma

Berikut ini adalah beberapa istilah yang digunakan dalam kriptografi [6] :

a) *Plaintext* adalah pesan asli yang nantinya akan digunakan atau dikirim ke pihak lain (berisi data asli).
b) *Ciphertext* adalah pesan yang sudah terenkripsi (tersandi) dan tidak bisa dibaca yang dimana hasil dari enkripsi.
c) Enkripsi adalah proses pengubahan data asli (*plaintext)* menjadi data yang suah dienkripsi atau disandikan (*ciphertext)*.
d) Dekripsi yakni merubah data yang sudah dienkripsi/disandikan (*ciphertext)* menjadi data asli kembali (*plaintext)*.
e) Kunci atau key adalah bilangan yang dirahasiakan dan digunakan dalam proses enkripsi dekripsi.

Teknik dasar algoritma kriptografi pun ada beberapa diantaranya adalah :

a) Metode Subtitusi
   Metode ini adalah sebuah metode yang dimana prosesnya menukar satu atau beberapa karakter ke yang lain.
b) Metode Block
   Metode ini digunakan dengan membagi plaintext ke blok-blok yang sudah sebelumnya dipecah ke beberapa karakter.
c) Metode Permutasi
   Metode ini proses nya dengan merotasikan karakter.

2.4. AlgoritmaAsimetris

Algoritma Asimetris adalah algoritma yang menggunakan 2 kunci , dimana dalam hal ini kunci sudah dibuat sebelumnya untuk poses enkripsi dekripsi informasi data. Algoritma ini disebut juga algoritma kunci umum (*pubic key algorithm)* karena kunci untuk proses enkripsi dibuat oleh siapa saja dan ingin menggunakan nya (*public key*) atau dapat diketahui oleh setiap orang, tapi kunci untuk proses dekripsi hanya diketahui oleh orang yang mengetahui data yang disandikan atau sering disebut kunci pribadi (*private key*)[1].

2.5. Algoritma Elgamal

Algoritma Elgamal merupakan algoritma kriptografi publik dan private yang dibuat oleh Taher ElGamal pada tahun 1984. Algoritma ini biasanya digunakan untuk proses digital signature, namun dimodifikasi juga bisa digunakan untuk proses mengamankan suatu informasi data. Kekuatan algoritma ini pada susahnya menghitung logaritma diskrit [5].

Tabel 1 : Hasil perhitungan proses enkripsi

i	m_i	k_i	$\gamma = 148^k \bmod 383$	$\delta = 295^k . m \bmod 383$
1	104	319	197	158
2	101	259	122	2
3	108	353	85	300
4	108	105	379	336
5	111	267	340	250
6	32	279	269	98
7	97	190	339	99
8	110	152	31	153
9	100	60	168	292
10	114	87	37	113
11	111	360	38	367
12	105	139	356	345
13	100	48	144	8

1. Susunlah plainteks menjadi blok-blok m_1, m_2, (nilai setiap blok di dalam selang $[0, p-1]$).
2. Pilih bilangan acak k, yang dalam hal ini $1 \leq k \leq p-2$.
3. Setiap blok m dienkripsi dengan rumus :
   $a = g^k \bmod p$
   $b = y^k m \bmod p$
4. Susun chipertext dengan urutan x1, y1, x2, y2, ..., an, bn.

Pasangan x dan y adalah cipherteks untuk blok pesan m. Jadi, ukuran cipherteks dua kali ukuran plainteksnya.

Diketahui: Plaintext: “hello android”

Nilai p = 383, g = 148, dan y = 295.

Nilai k1 = 319, k2 = 259, k3 = 353, k4 = 105, k5 = 267, k6 =279, k7 = 190, k8 = 252, k9 = 60, k10 = 87, k11 = 360, k12 =139

Tabel 2 :Hasil perhitungan proses dekripsi

i	δ	γ	$m_i = \delta_i . \gamma_i^{(383-1-338)} \bmod 383$	Karakter m_i
1	158	197	104	h
2	2	122	101	e
3	300	85	108	l
4	336	379	108	l
5	250	340	111	o
6	98	269	32	<spaci>
7	99	339	97	a
8	153	31	110	n
9	292	168	100	d
10	113	37	114	r
11	367	38	111	i
12	345	356	105	o
13	8	144	100	d

Pada proses ini digunakan kunci pribadi (x, p).

1. Gunakan kunci privat *x* untuk menghitung plaintext m = $a.b^{(p-1-x)} \bmod p$
2. Nilai m yang didapat dalam ASCII lalu diubah menjadi plaintext.
3. Susunlah plaintext dengan urutan m1, m2, m3, ..., mn.

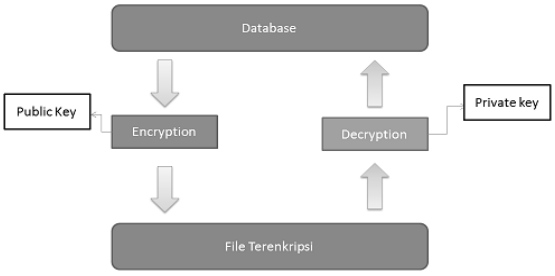
Hasil yang didapat dari proses dekripsi berupa pesan asli (plaintext). Langkah penyelesaian dekripsi secara manual adalah sebagai berikut:

Ciphertext : 197, 158, 122, 2, 85, 300, 379,336, 340, 250, 269, 98, 339, 99, 31, 153, 168,292, 37, 113, 38, 367, 356, 345, 144, 8
Nilai p = 383, x = 338.

3. RANCANGAN SISTEM DAN APLIKASI

3.1. Arsitektur Sistem

Program yang akan dibuat terdiri dari beberapa *Form,* yaitu terdiri dari *Form Login,* Menu Utama, *Transaksi,* Generate Key, Enkripsi, Dekripsi, Master Barang, Master Customer, *Profile, dan Help.* Untuk dapat melakukan enkripsi *database* pengguna dapat menggunakan *button* enkripsi pada *form enkripsi* yang sebelumnya sudah memiliki kunci publik untuk prosesnya. Sedangkan untuk mengembalikan di *database* yang sudah terenkripsi menjadi *database* asli, pada *form dekripsi* yang dimana sudah memiliki kunci private untuk prosesnya .

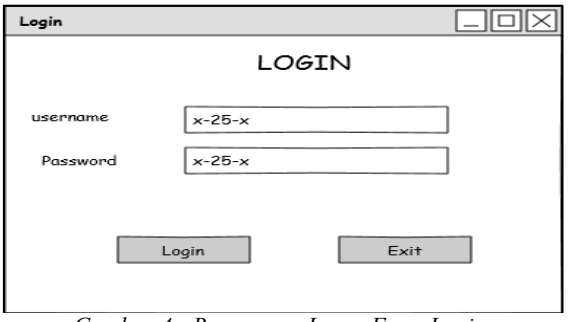


Gambar 3 : Arsitektur Aplikasi

3.2. Rancangan Layar

3.2.1. *Form* Menu Login

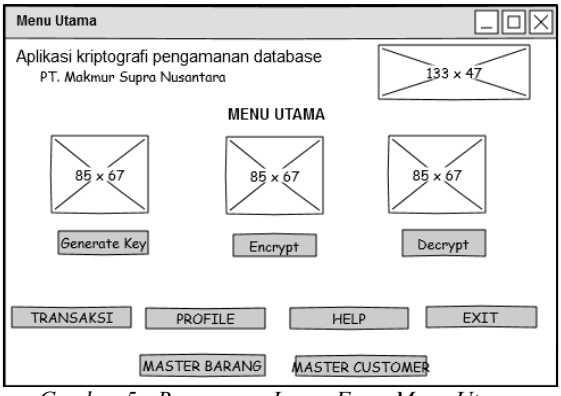
Form Login adalah tampilan awal saat program diakses, berfungsi sebagai sebuah akses menuju ke menu utama. Pada gambar di bawah ini disediakan menu pengisian *username* dan *password*. Bila *username* dan *password* sesuai maka langsung menuju ke menu utama.



Gambar 4 : Rancangan Layar Form Login

3.2.2. Rancangan Layar *Form* Menu Utama

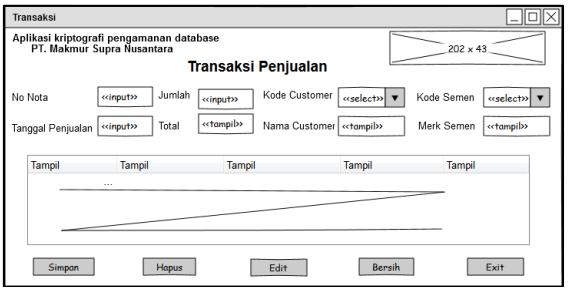
Setelah *login* berhasil, *user* akan masuk ke dalam *form* menu utama aplikasi. Jika *user* ingin melakukan *entry* data *transaksi, user* dapat memilih *button transaksi* pada form menu utama. Jika user ingin *entry* barang, *user* dapat memilih tombol master barang pada form menu utama. Jika *user* ingin *entry* data customer, *user* dapat memilih tombol master customer pada form menu utama. Dan jika *user* ingin melakukan proses enkripsi dan dekripsi maka user menekan tombol *encrypt* dan *decrypt.* Dan tersedia juga tombol help untuk melihat cara penggunaan program. Seperti gambar berikut ini:



Gambar 5 : Rancangan Layar Form Menu Utama

3.2.3. Rancangan Layar *Form Transaksi*

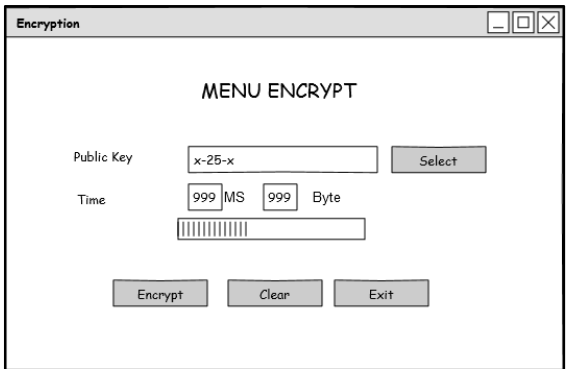
Pada rancangan menu *Form Transaksi,* berfungsi untuk melakukan *input,* simpan, *edit,* dan hapus data *transaksi*. Seperti gambar berikut ini:



Gambar 6: Rancangan Layar Form Transaksi

3.2.4. Rancangan Layar *Form* Encrypt

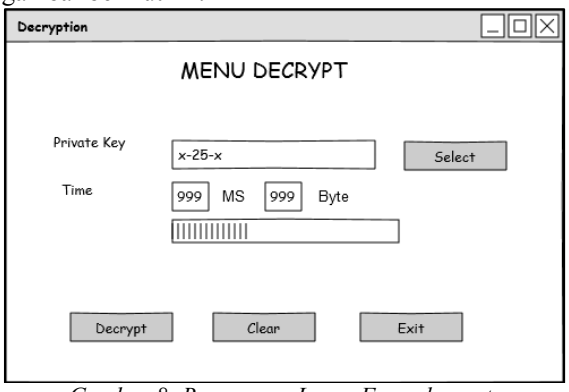
Pada rancangan menu *Form* Encrypt, berfungsi untuk melakukan proses enkripsi data di dalam database yang sebelumnya sudah memiliki kunci publik. Seperti gambar berikut ini:



Gambar 7:Rancangan Layar Form Encrypt

3.2.5. Rancangan Layar *Form*Decrypt

Pada rancangan menu *Form decrypt,* berfungsiuntuk melakukan proses dekripsi data di dalam database yang sebelumnya sudah terenkripsi dan memiliki kunci private untuk prosesnya. Seperti gambar berikut ini:

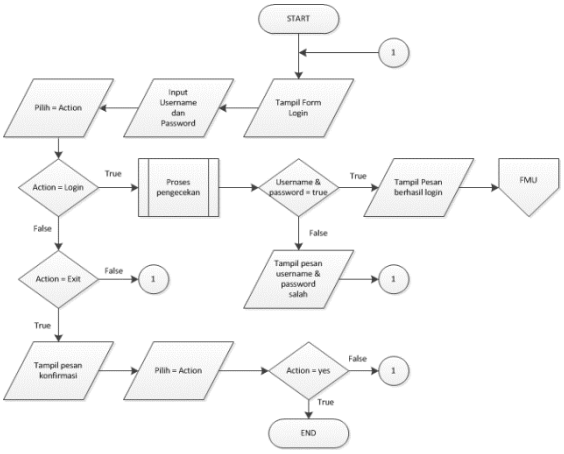


Gambar 8: Rancangan Layar Form decrypt

3.3. Flowchart

3.3.1. Flowchart *Form Login*

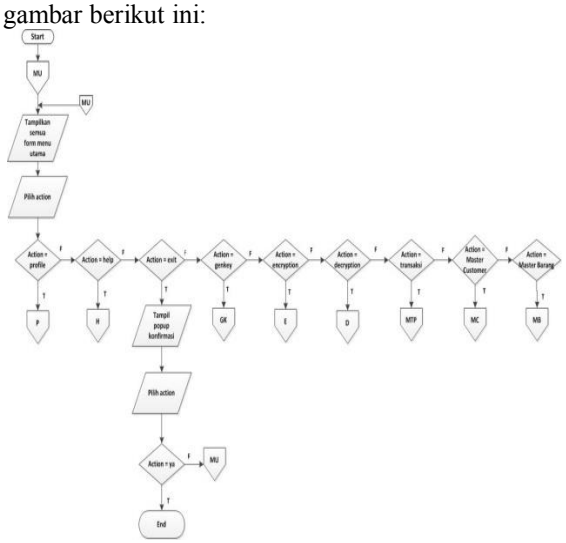
Pada *flowchart* ini dijelaskan tentang bagaimana *user login* untuk menggunakan aplikasi ini. *User* terlebih dahulu menginput *username* dan *password.* Jika *username* dan *password* yang diinput tidak sesuai maka akan tampil *messagebox* yang isinya menginformasikan bahwa *login* gagal dan *user* dikembalikan kembali ke *form login* untuk mengisi kembali *username* dan *password* dengan sesuai. Seperti gambar berikut ini :



Gambar 9 : Flowchart Form Login

3.3.2. Flowchart *Form* Menu Utama

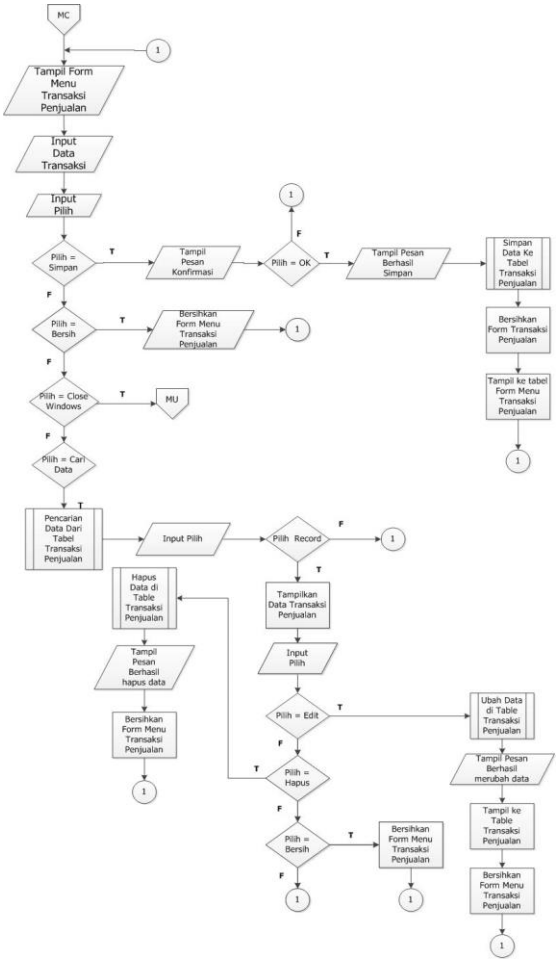
Flowchart ini menjelaskan proses tampilan di menu utama untuk dapat masuk ke menu lain yang diinginkan pengguna, di dalam menu utama terdapat tombol-tombol yang digunakan untuk proses input data dan proses enkripsi dan dekripsi. Seperti gambar berikut ini:



Gambar 10 : Flowchart Form Menu Utama

3.3.3 Flowchart *Form Transaksi*

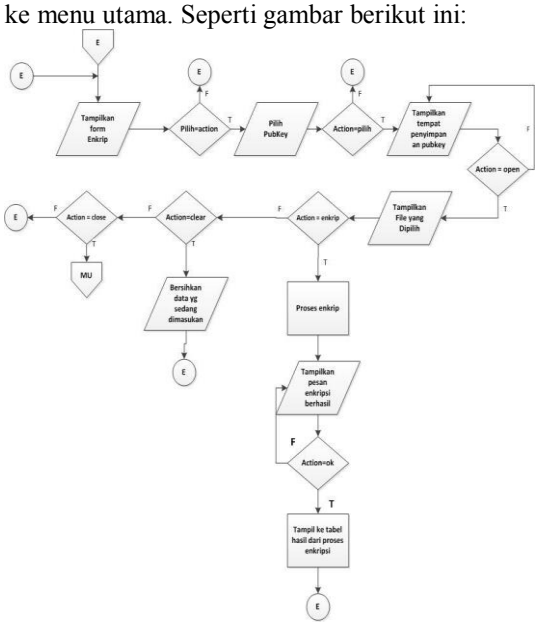
Flowchart form transaksi merupakan gambaran alur proses dari *form transaksi*. Pada proses ini *user* dapat menyimpan, edit, dan hapus data *transaksi.* Jika *user* memilih tombol simpan, maka data yang diinput oleh *user* akan tersimpan. Jika user memilih tombol edit, maka data akan berubah. Jika *user* memilih tombol bersih maka data yang tampil pada *textfield* di menu akan hilang, dan apabila *user* memilih tombol *back* maka akan kembali lagi ke menu utama. Seperti gambar berikut ini:



Gambar 11 : Flowchart Form Transaksi

3.3.4. Flowchart *Form* Encrypt

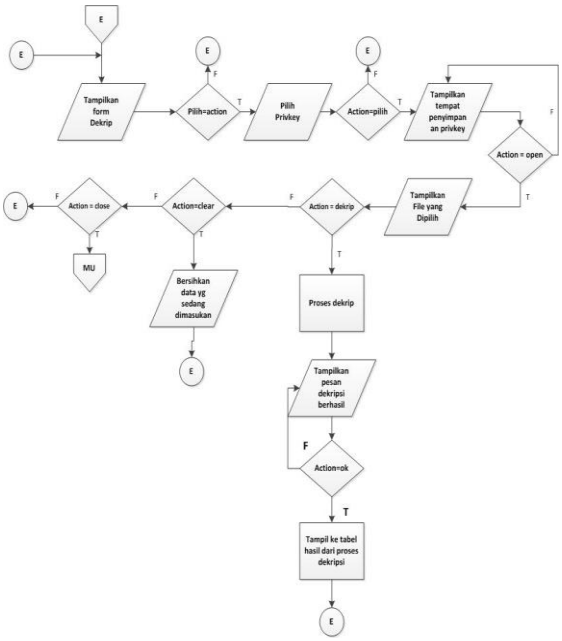
Flowchart form encrypt merupakan gambaran alur proses dari *form* encrypt. Pada proses ini *user* dapat melakukan proses enkripsi dengan memilih public key yang sebelumnya sudah dibuat. Dan jika *user* memilih tombol *back* maka akan kembali lagi ke menu utama. Seperti gambar berikut ini:



Gambar 12: Flowchart Form Encrypt

3.3.5 Flowchart *Form* Decrypt

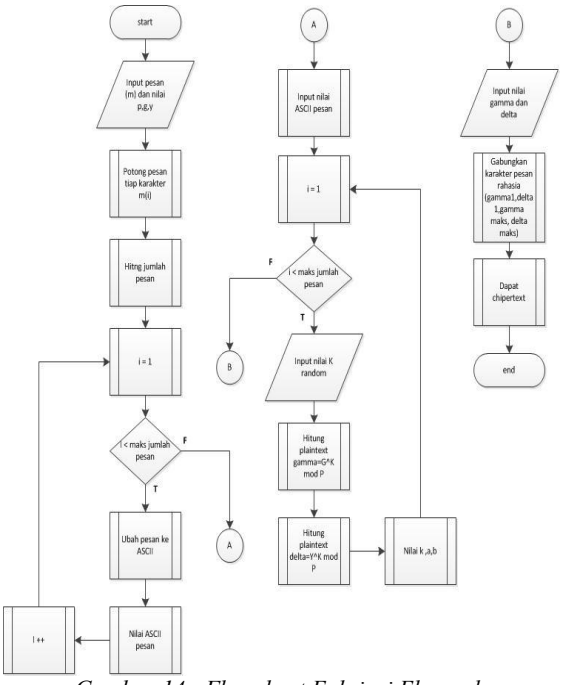
Flowchart form decrypt merupakan gambaran alur proses dari *form* decrypt. Pada proses ini *user* dapat melakukan proses dekripsi dengan memilih private key yang sebelumnya sudah dibuat. Dan jika si *user* memilih tombol *back* maka akan kembali lagi ke menu utama. Seperti gambarberikut ini:



Gambar 13 : Flowchart Form Decrypt

3.3.6 Flowchart Enkripsi Elgamal

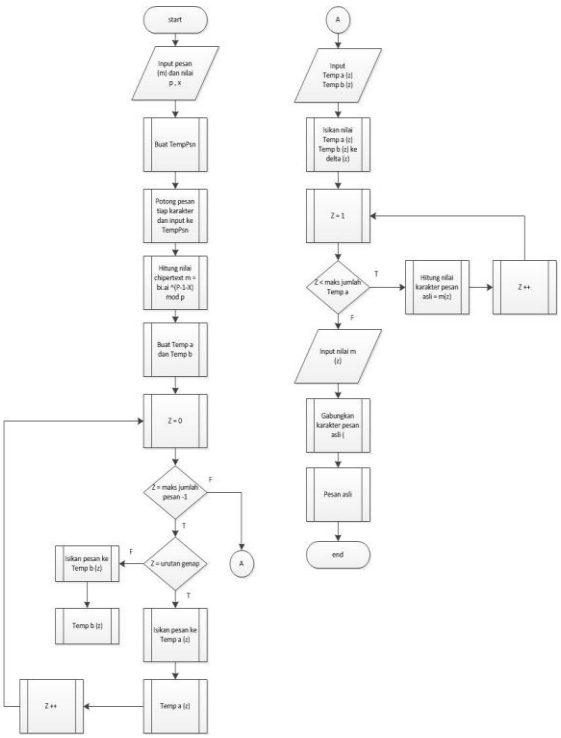
Flowchart ini menjelaskan proses adanya mengubah plaintext ke ciphertext dengan menggunakan algoritma Elgamal. Seperti gambar berikut ini:



Gambar 14 : Flowchart Enkripsi Elgamal

3.3.7 Flowchart Dekripsi Elgamal

Flowchart ini menggambarkan proses pengembalian ciphertext ke plain text dengan algoritma Elgamal. Seperti gambar berikut ini:



Gambar 15 : Flowchart Dekripsi Elgamal

4. HASIL DAN PEMBAHASAN

4.1. Tampilan Layar *Form Login*

Tampilan layar *form Login* di gambar di bawah ini muncul pertama saat program dijalankan, yang berisi *textbox* dan *button* untuk *login* ke dalam aplikasi dan *exit* untuk keluar dari aplikasi.

Gambar 16 : Tampilan Layar Form Login

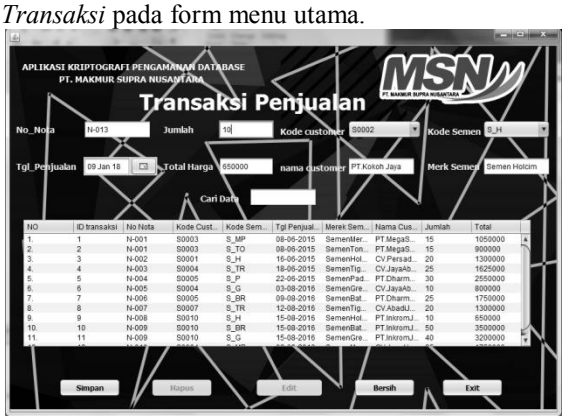
4.2. Tampilan Layar *Form*Menu Utama

Tampilan layar dari form Menu Utama pada gambar ini muncul setelah pengguna berhasil login ke dalam aplikasi, Form ini berisi beberapa menu yang digunakan seperti: Generate Key, Master Transaksi, Master Barang, Master Customer, Encrypt, Decrypt, Profile, Help, dan Exit untuk keluar dari program.

Gambar 17 : Tampilan Form Menu Utama

4.3. Tampilan Layar *FormTransaksi*

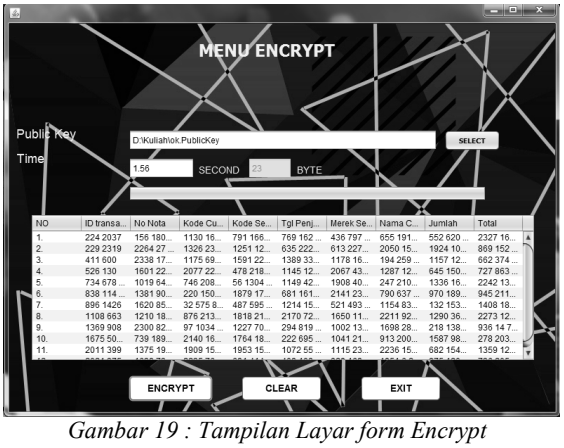
Tampilan layar *form Transaksi* pada gambar di bawah ini terlihat pada saat user mengklik tombol *Transaksi* pada form menu utama.



Gambar 18: Tampilan Layar Form Transaksi

4.4. Tampilan Layar *FormEncrypt*

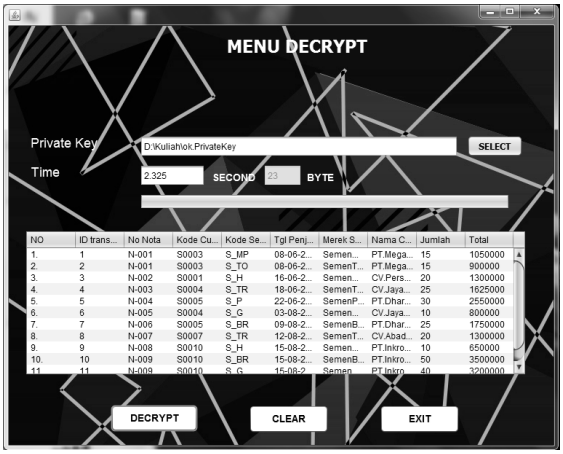
Tampilan layar *form Encrypt* pada gambar di bawah ini terlihat pada saat user mengklik tombol *encrypt* pada form menu utama.



Gambar 19 : Tampilan Layar form Encrypt

4.5. Tampilan Layar *Form Decrypt*

Tampilan layar *form Decrypt* pada gambar di bawah ini terlihat pada saat user mengklik tombol *decrypt* pada form menu utama.



Gambar 20 : Tampilan Layar form Decrypt

4.4. Hasil Pengujian

4.4.1 Hasil Pengujian Tabel *Transaksi*

Berikut ini adalah hasil pengujian pada proses enkripsi *database* yang telah diuji.

Tabel 3: Hasil Pengujian Enkripsi Tabel Transaksi

Nama Data tabel	Size data enkripsi	Waktu (S)	Jumlah data record	Status	genkey
Data_transaksi penjualan	144 kb	6.069	50	Berhasil	Ok.pub
Data_transaksi penjualan	176 kb	13.075	100	Berhasil	Ok.pub
Data_transaksi penjualan	224 Kb	15.401	150	Berhasil	Ok.pub

Tabel 4: Hasil Pengujian Dekripsi Tabel Transaksi

Nama Data tabel	Size data dekripsi	Waktu (S)	Jumlah data record	Status	genkey
Data_transaksi penjualan	144 kb	157.734	50	Berhasil	Ok.priv
Data_transaksi penjualan	176 kb	313.408	100	Berhasil	Ok.priv
Data_transaksi penjualan	224 KB	486.51	150	Berhasil	Ok.priv

4.5 Evaluasi Program

Setelah melakukan analisa dan penelitian dari hasil pengujian program, maka dapat ditemukan kelebihan dan kekurangannya dari program ini, yaitu sebagai berikut:

a. Kelebihan Program

1) Tampilan intefacenya yang menarik.
2) *Database* yang dienkripsi tidak bisa dibaca lagi.
3) Isi dalam tabel *database* tidak adanya perubahan setelah didekripsi.

b. Kekurangan Program

1) Aplikasi ini hanya dapat mengenkripsi dan mendekripsi *database* per-*table.*
2) Waktu yang diperlukan untuk proses dekripsi masih terbilang kurang cepat.
3) Semakin banyak data di dalam database maka prosesnya akan semakin lama.
4) Semakin besar ukuran sebuah database maka proses nya akan semakin lama.
5) Saat proses enkripsi dan dekripsi waktu proses selalu berbeda

5. KESIMPULAN

5.1. Kesimpulan

Adapun kesimpulan yang bisa diperoleh perancangan, serangkaian uji coba dan analisa program ini dapat beberapa kesimpulan sebagai berikut ini :

a. Dengan dibuatnya program ini, proses penyimpanan data ke database menjadi aman.
b. Aplikasi ini dapat mengamankan data di dalam database dengan teknik kriptografi menggunakan metode algoritma Elgamal.
c. Algoritma Elgamal dapat diterapkan penggunaaanya pada aplikasi pengamanan database.

5.2. Saran

Ada beberapa saran yang mungkin dibutuhkan untuk membuat program ini jadi lebih baik lagi, antara lain :

a. Dilakukan pelatihan terlebih dahulu kepada user agar user dapat memahami cara penggunaan program tersebut.
b. Aplikasi ini diharapkan ke depannya dapat mengenkripsi per record ataupun per column.
c. Program atau perangkat lunak ini dapat dikembangkan lebih baik.

DAFTAR PUSTAKA

[1] Kromodimoeljo, S. (2010). *Teori & Aplikasi Kriptografi*, 1(1) 1-453. Diterbitkan oleh: SPK IT Consulting, Desember.

[2] Hasrul, H., & Siregar, L. H. (2016). Penerapan Teknik Kriptografi Pada Database Menggunakan Algoritma One Time Pad, 2(2), 41–52.

[3] Ariyus, Donny. 2008. Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi. Yogyakarta: Andi offset.

[4] Irmansyah, Faried. 2013. Dasar-Dasar Algoritma dan Pemrograman. Yogyakarta: Andi Offset.

[5] Kurniadi, A. (2016). Implementasi Kriptografi Elgamal dalam Keamanan Pesan, Jurnal Infotek, Februari, 1(1), 1–5. STMIK Budidarma Medan.

[6] Munir, U. S. (2006). Universitas Sumatera Utara. Retrieved from http://repository.usu.ac.id/bitstream/123456789/43370/4/Chapter II.pdf.