# APLIKASI PENGAMAN BASIS DATA PADA NUKLINDO LAB DENGAN ALGORITMA ELGAMAL DAN AFFINE CIPHER

**Albi Dwi Haryono**[1)], **Pipin Farida Ariyani**[2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : alber9193@gmail.com[1)], pipin.faridaariyani@budiluhur.ac.id[2)]

***Abstrak***

*Nuklindo Lab merupakan salah satu unit usaha Koperasi Jasa Keselamatan Radiasi dan Lingkungan (JKRL) yang bergerak di bidang pelayanan jasa keselamatan dan kesehatan kerja (K3) dan lingkungan baik radiasi maupun non radiasi yang memiliki database yang berisi data intansi, data pekerja, data rumus dan data evaluasi dosis. Sering sekali record yang tersimpan di dalam database masih teks berupa asli. Hal ini bisa mempermudah orang yang tidak mempunyai wewenang dapat mengetahui langsung isi dari record database tersebut serta dapat memberi peluang kepada mereka untuk melakukan pembocoran, mendistribusikan maupun melakukan modifikasi lain terhadap isi dari database tersebut. Oleh karena itu dibutuhkan aplikasi yang dapat memudahkan pengguna untuk menginput dan menyimpan data tersebut dengan aman dan terjaga kerahasiaannya. Pada penelitian ini implementasi pengamanan data dari sisi kandungan data yang tersimpan pada database. Teknik pengamanan data ini dilakukan dengan menggunakan teknik kriptografi Elgamal Karena Keamanan Elgamal terletak pada sulitnya menghitung logaritma diskrit dan Affine Cipher dipilih Karena perluasan dari metode Caesar Cipher. Hasil dari penelitian ini mempunyai kelebihan record database dienkripsi sangat tinggi karena menggunakan 2 metode kriptografi, yaitu Elgamal dan Affine Cipher sehingga sangat sulit untuk dibaca isi record tersebut serta kekurangannya hasil text hasil enkripsi bertambah panjang.*

**Kata kunci:** Kriptografi , Elgamal, *Affine Cipher, Database.*

## 1. PENDAHULUAN

Dengan perkembangan teknologi informasi dan komunikasi yang berkembang sangat pesat. Namun juga dibarengi dengan tuntutan keamanan dan kerahasiaan informasi yang disampaikan. Oleh karena itu, keamanan data merupakan aspek utama yang ada didalam sistem operasi komputer yang kini telah menjadi suatu alat bantu utama dalam kehidupan manusia sehari-hari. Berdasarkan permasalahan tersebut timbul sebuah gagasan penulis melakukan riset pada Nuklindo Lab yang memiliki *database* yang berisi data besifat rahasia seperti data intansi, data pekerja, data rumus dan data evaluasi dosis. Sering sekali *record* yang tersimpan di dalam *database* masih persis sama dengan teks yang ditampilkan sebagai informasi akhir bagi pengguna.

Hal ini bisa mempermudah orang yang tidak mempunyai wewenang dapat mengetahui langsung isi dari record *database* tersebut serta dapat memberi peluang kepada mereka untuk melakukan pembocoran. Dalam merealisasikannya penulis akan membuat aplikasi pengamanan basis data dengan bahasa pemrograman java beserta *database* MySQL yang diguakan dalam penyimpanan data. Sehingga Nuklindo Lab dapat mengamankan *record* yang tersimpan di dalam *database*, maka pengamanan data dapat dilakukan dengan menggunakan teknik Kriptografi.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data[1]. Data/ informasi tersebut harus tetap rahasia selama disimpan dan harus tetap terjaga kerahasiannya. Kriptografi memiliki 2 tahap yaitu proses enkripsi dan dekripsi Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi ciphertext. Sedangkan proses yang dilakukan untuk mengubah pesan tersembunyi menjadi pesan biasa (yang dapat dibaca dan dimengerti) disebut dekripsi[2]. Selain itu tujuan penelitian ini yaitu mengimplementasikan algoritma Elgamal dan algoritma *Affine Cipher.* Adapun batasan dalam aplikasi ini yaitu data yang akan dienkripsi dan didekripsi pada aplikasi ini adalah data instansi, pekerja, rumus dan evaluasi dosis yang ada pada Nuklindo Lab, dan Aplikasi *Database Management System* yang digunakan *MYSQL.*

## 2. METODE PENELITIAN

Dalam penelitian ini, penulis menggunakan metode model *Software Development Life Cycle* (SLDC) yaitu metode *Waterfall* tahapan SLDC dengan metode waterfall meliputi tahapan perencanaan, analisis, desain, implementasi, pengujian dan pemeliharaan. Berikut ini adalah rincian tahapan dalam pembuatan aplikasi :

a. Pengumpulan Data dari keseluruhan elemen sistem yang akan diaplikasikan ke dalam bentuk *software* atau perangkat lunak dan mengumpulkan data mengenai sistem *database* di Nuklindo Lab enkripsi *database,* serta algoritma Elgamal dan algoritma *Affine Cipher.*

b. Menganalisa Kebutuhan Aplikasi kemudian dipelajari dan dianalisa mengenai fungsi-fungsi apa saja yang diperlukan untuk mengimplementasikan aplikasi ini.
c. Desain atau Perancangan Program tampilan aplikasi yang akan dibangun sesuai dengan kebutuhan aplikasi sehingga dapat mempermudah dalam proses pengkodean.
d. Pengkodean dilakukan untuk memudahkan dalam mengimplementasikan rancangan aplikasi ke dalam algoritma Elgamal dan algoritma *Affine Cipher* dengan menggunakan bahasa pemrograman Java.
e. Implementasi berdasarkan analisa masalah.
f. Testing atau pengujian dilakukan setelah aplikasi selesai dibuat dengan melakukan beberapa pengujian progam dan mencari kesalahan pada program hingga tidak ada lagi kesalahan program dan program sudah berjalan sesuai dengan yang dirancang.

### 2.1. Algoritma Elgamal

Algoritma ElGamal ditemukan oleh ilmuwan Mesir, yaitu Taher ElGamal pada tahun 1985, merupakan algoritma kriptografi kunci publik[3].

**a. Proses Generate Key Elgamal**

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 sebagai berikut[4] :

$$Y = (g^x) \bmod p$$

**b. Proses Enkripsi Elgamal**

Proses enkripsi merupakan proses mengubah pesan asli (*plaintext)* menjadi pesan rahasia (*ciphertext)*. Pada proses ini digunakan kunci *public* (p,g,y). langkah – langkah dalam mengenkripsi pesan adalah pada persamaan sebagai berikut [4]:

$$a = (g^k) \bmod p$$

$$b = (y^{k.m}) \bmod p$$

**c. 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 berikut [4]:

$$m = b.a^{(p-1-x)} \bmod p$$

### 2.2 Algoritma Affine Cipher

Secara matematis enkripsi *plainteks* menghasilkan *cipherteks* dinyatakan fungsi kongruen pada persamaan berikut[5]:

$$C(P) = (aP+b) \bmod n$$

Untuk memperoleh kembali plaintext maka fungsi dekripsi harus diperoleh terlebih dahulu.

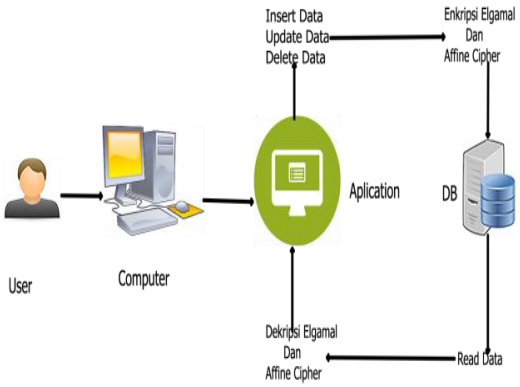
$$C(P) = a\text{-}1(C-b) \bmod n$$

## 3. RANCANGAN SISTEM DAN APLIKASI

Aplikasi pengamanan database ini dirancang dengan berbagai fitur yaitu menginput, mengubah, menghapus ataupun melihat data yang sudah di enkripsi pada data instansi, pekerja, rumus ,dan evaluasi

### 3.1. Arsitektur Sistem

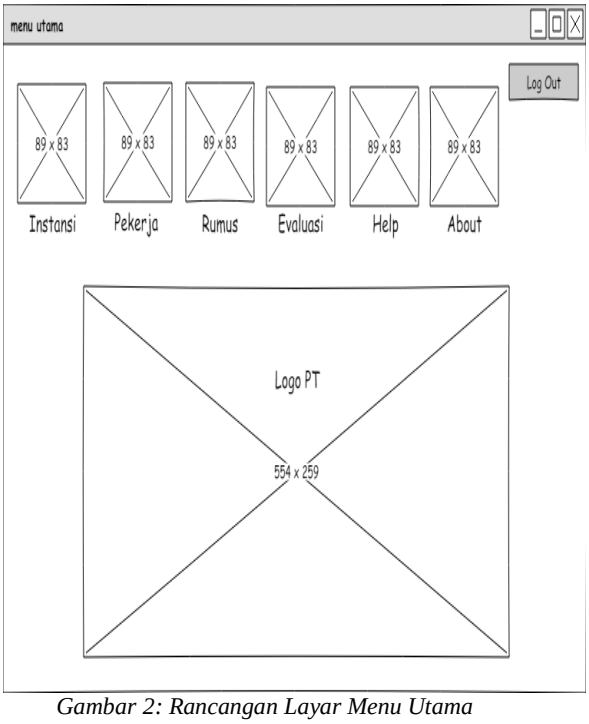
Berikut ini merupakan arsitektur aplikasi, untuk dapat memahami konsep aplikasi yang akan dibangun dapat melihat pada gambar 1. Pada gambar arsitektur aplikasi menggambarkan secara garis besar proses dari keseluruhan sistem.




*Gambar 1: Arsitektur Sistem*

### 3.2. Rancangan Layar *Menu* Utama

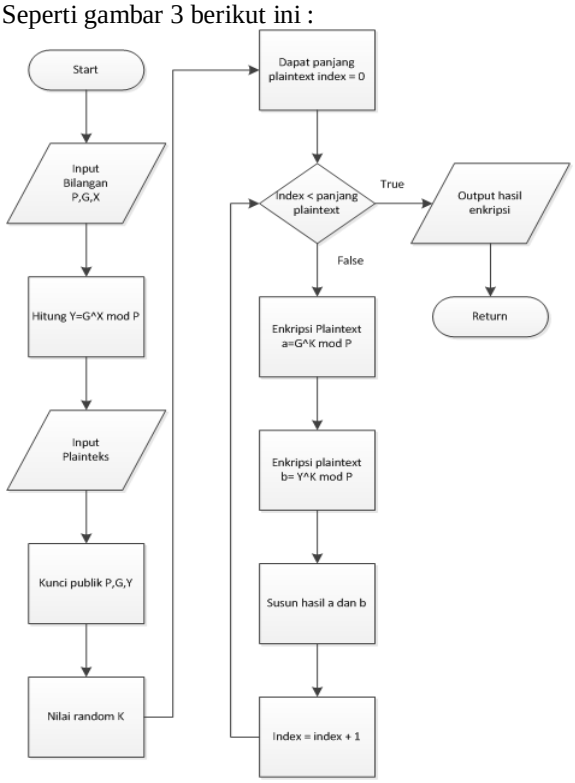
*Menu* ini adalah *menu* utama dimana pengguna dapat milih data apa yang akan dienkripsi dan didekripsi untuk disimpan ke dalam *database,* terlihat seperti gambar 2 berikut ini :




*Gambar 2: Rancangan Layar Menu Utama*

### 3.3. *Flowchart* Enkripsi Elgamal

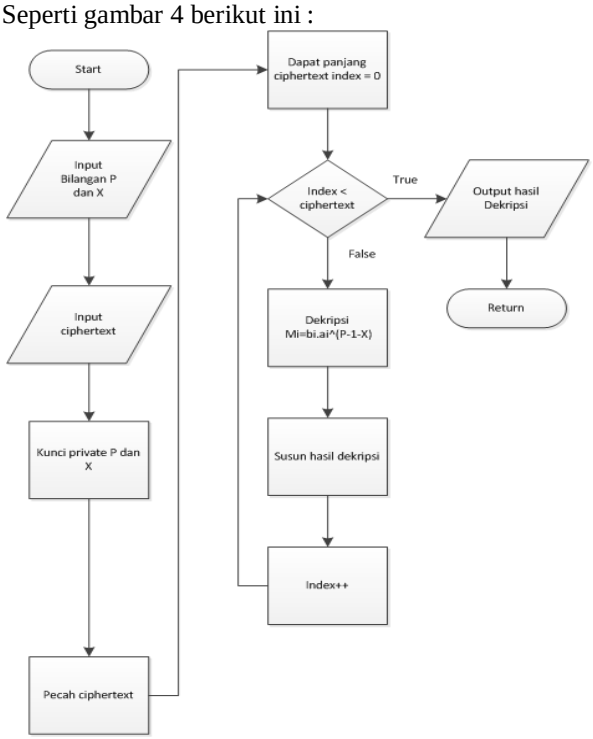
*Flowchart* proses enkripsi Elgamal merupakan gambaran alur yang akan mengalami proses enkripsi Seperti gambar 3 berikut ini :




*Gambar 3: Flowchart Enkripsi Elgamal*

### 3.4. *Flowchart* Dekripsi Elgamal

*Flowchart* proses dekripsi Elgamal merupakan gambaran alur yang akan mengalami proses dekripsi Seperti gambar 4 berikut ini :




*Gambar 4: Flowchart Deskripsi Elgamal*

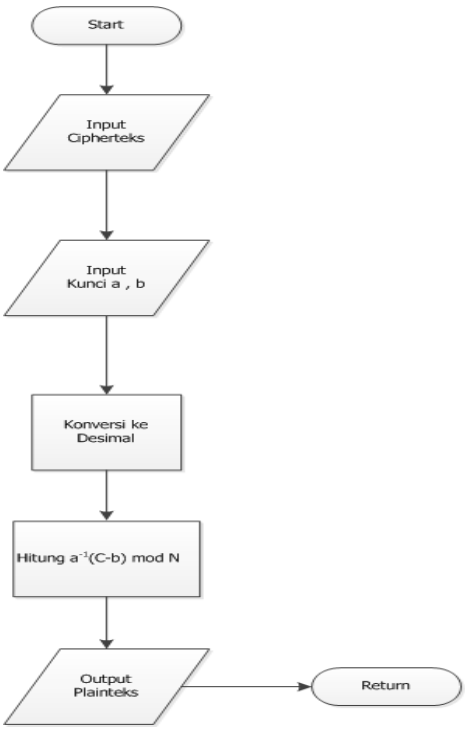
### 3.5. *Flowchart* Enkripsi Affine *Cipher*

*Flowchart* proses *enkripsi affine cipher* merupakan gambaran alur yang akan mengalami proses enkripsi Seperti gambar 5 berikut ini :


*Gambar 5: Flowchart Enkripsi Affine Cipher*

### 3.6. *Flowchart* Deskripsi Affine *Cipher*

Flowchart proses dekripsi *affine cipher* merupakan gambaran alur yang akan mengalami proses dekripsi Seperti gambar 6 berikut ini :




*Gambar 6: Flowchart Deskripsi Affine Cipher*

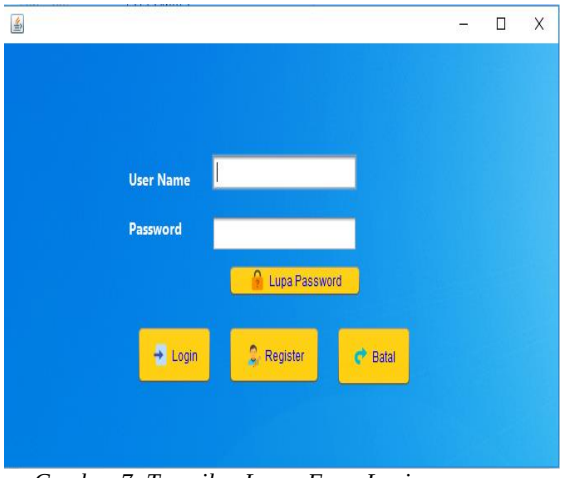
## 4. HASIL DAN PEMBAHASAN

### 4.1. Tampilan Aplikasi

Tampilan aplikasi berikut ini merupakan tampilan form fungsi utama yang digunakan dari aplikasi ini.

**a. Tampilan Layar *Form Login***

Tampilan awal pada saat aplikasi dibuka adalah *Form Login*, pengguna harus memasukkan *username* dan *password* yang sudah dimiliki terlebih dahulu. jika *password* benar maka login berhasil. Setelah *login* berhasil, maka pengguna akan menuju halaman menu utama Rancangan layar *Form login*. Bentuk tampilannya pada gambar 7.




*Gambar 7: Tampilan Layar Form Login*

**b. Tampilan Layar *Menu Utama***

Tampilan Menu Utama akan muncul ketika pengguna berhasil melakukan *login*. Pada Menu Utama terdapat 6 Form yaitu *Form Instansi*, Pekerja, Rumus, Evaluasi, *Help*, *About*. Tampilan layar *Main Menu* dapat dilihat pada gambar 8 berikut ini:


*Gambar 8: Tampilan Layar Main Menu*

**c. Tampilan Layar *Form* Instansi**

Tampilan ini akan muncul ketika user memilih *Form* Instansi, *Form* Instansi berfungsi untuk menginput, mengubah, menghapus ataupun melihat data Instansi dapat dilihat pada gambar 9 .

*Gambar 9: Tampilan Layar Form Instansi*

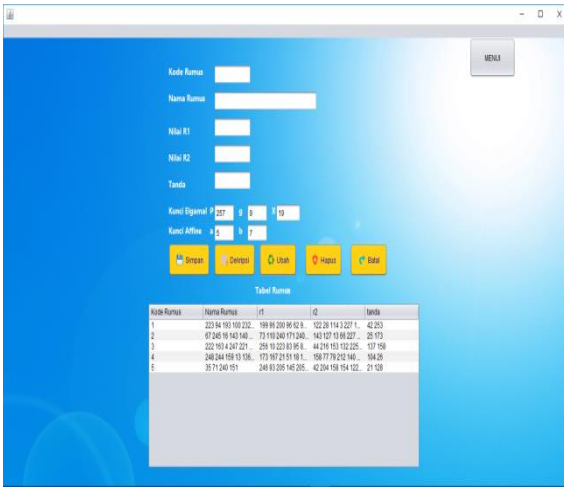
**d. Tampilan Layar *Form* Pekerja**

Tampilan ini akan muncul ketika user memilih *Form* Pekerja, *Form* pekerja berfungsi untuk menginput, mengubah, menghapus ataupun melihat data pekerja dapat dilihat pada gambar 10 berikut ini :

*Gambar 10: Tampilan Layar Form Pekerja*

**e. Tampilan Layar *Form* Rumus**

Tampilan ini akan muncul ketika user memilih *Form* Rumus, *Form* Rumus berfungsi untuk menginput, mengubah, menghapus ataupun melihat data Rumus dapat dilihat pada gambar 10 berikut ini :



*Gambar 11: Tampilan Layar Form Rumus*

**f. Tampil Layar *Form* Evaluasi**

Tampilan ini akan muncul ketika user memilih *Form* Evaluasi, *Form* Evaluasi berfungsi untuk menginput, mengubah, menghapus ataupun melihat data Evaluasi dapat dilihat pada gambar 11 berikut ini :


*Gambar 11: Tampilan Layar Form Evaluasi*

## 4.2. Tabel Pengujian

Pengujian ini dilakukan untuk mengetahui panjang dari teks yang dihasilkan dari proses enkripsi dan dekripsi menggunakan metode Elgamal dan *Affine cipher* membandingkannya dengan panjang teks aslinya.

*Tabel 1: Tabel Pengujian*

| Nama Data | Karater Asli | jumlah | Karakter Hasil Enkripsi | Jumlah Karakter Hasil Enkripsi | Waktu |
|---|---|---|---|---|---|
| Nama Instansi | RS. HERMINA PANDANARAN | 22 | 114 220 246 101 18 119 226 87 213 136 165 125 165 132 26 59 62 246 168 128 211 3 249 77 46 38 157 97 136 236 246 156 79 171 118 8 9 27 8 192 9 27 84 16 58 153 111 175 118 188 187 165 84 226 100 | 251 | 0.0034 |
| | | | 68 52 232 59 4 81 125 32 156 215 23 13 146 235 66 249 110 | | |
| Alamat | Jl. Pandanaran No. 24 semarang | 30 | 128 17 187 1 241 194 165 188 4 155 135 44 173 148 60 206 196 134 139 74 117 98 23 28 116 32 231 160 139 109 89 129 146 226 208 229 26 63 57 159 139 178 187 181 92 32 221 0 249 80 22 31 121 212 26 246 64 180 176 54 9 79 134 39 213 177 162 67 246 165 205 222 31 168 208 70 92 105 92 172 79 46 226 22 23 94 1 55 | 309 | 0.041 |
| Kontak | 02484 42525 | 10 | 95 82 234 134 159 226 67 159 246 200 57 207 70 242 124 79 8 | 179 | 0.006 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 225 26 25 215 18 239 139 68 177 4 39 144 232 236 133 46 18 64 128 187 185 168 39 120 142 240 185 118 129 242 3 153 151 | | |
| email | pandanaran@hermina hospitalgroup.com | 35 | 73 166 49 235 42 110 135 86 21 15 29 54 31 211 146 191 253 59 241 206 225 93 104 99 195 0 121 212 178 167 190 230 79 37 248 92 72 199 146 226 22 68 57 7 22 203 244 119 98 81 36 133 120 166 35 243 100 227 139 103 88 5 253 252 240 184 234 18 221 105 18 118 121 126 228 33 144 232 135 141 1 58 36 173 52 234 49 80 235 20 29 | 343 | 0.024 |
| | | | 213 95 98 11 56 221 48 | | |
| | Rata - Rata | 24.25 | | 270.5 | 0.027 |

### 4.3 Evalusi Program

Setelah dilakukan Analisa dari hasil pengujian aplikasi maka dapat ditemukan beberapa kelebihan dan kekurangannya dari aplikasi ini, yaitu sebagai berikut:

a. Kelebihan Program
   1) Terdapat autentikasi *Username* dan *Password* pada *Form Login.*
   2) Program yang *user friendly*, karena memilik tampilan yang sederhana dan jelas.
   3) Keamanan *database* yang telah dienkripsi sangat tinggi karena menggunakan 2 metode kriptografi, yaitu Elgamal dan *Affine Cipher*.

b. Kekurangan Program
   1) Tidak bisa diakses dimana saja karena tidak berbasis website.
   2) Aplikasi hanya dapat digunakan pada database yang sudah ditentukan oleh *user*.
   3) Aplikasi ini hanya dapat mengenkripsi dan dekripsi *database* per record dalam satu kali proses.
   4) Hasil text asli ke enkripsi bertambah panjang.

## 5. KESIMPULAN

### 5.1 Kesimpulan

Berdasarkan hasil analisa yang telah kami lakukan terhadap permasalahan dan aplikasi yang dikembangkan, maka dapat ditarik suatu kesimpulan, sebagai berikut:

a. Enkripsi Elgamal dan *Affine Cipher* ini dapat diimplementasikan pada aplikasi pengamanan *database* dengan menggunakan bahasa pemrograman Java dan *database* MySQL.
b. Aplikasi ini dapat mengamankan data yang masuk kedalam database dengan teknik kriptografi menggunakan metode Elgamal dan *Affine Cipher* sehingga data yang tersimpan kedalam *database* akan sulit untuk dibaca.
c. Aplikasi ini dapat dijalankan sesuai dengan spesifikasi teknis yang dirancang.

### 5.2 Saran

Selain menarik beberapa kesimpulan, dapat pula diajukan saran-saran yang mungkin bisa dijadikan pertimbangan dalam pengembangan sistem, antara lain:

a. Diharapkan dilakukan pelatihan terlebih dahulu kepada *user* agar *user* benar-benar memahami sistem dan cara penggunaannya sekaligus pemeliharaannya sehingga sistem dapat

digunakan dengan optimal untuk jangka waktu yang lama.

b. Interface masih sangat sederhana, diharapkan bisa ditambah beberapa fitur seperti progres bar dan waktu lama proses enkripsi dan dekripsi.

c. Program atau perangkat luna ini dapat dikembangkan dengan menambahkan penjelasan yang lebih detail dan lebih baik

## 6. DAFTAR PUSTAKA

[1] Triase , 2015, Kriptografi Elgamal Menggunakan Metode Mersenne, Jurnal ilmiah "INTEGRITAS" Vol.1.

[2] Gea Firman , 2016, Perancangan Aplikasi Enkripsi Pesan Singkat Dengan Menggunakan Algoritma Affine Cipher Dan Vigenere Cipher Berbasis Android, Jurnal Infotek STIEKOM, hal 30-39.

[3] Rochmat N, Isnanto R R, & Somantri M, 2012, Implementasi Algoritma Kriptografi Elgamal Untuk Keamanan Pesan ( Message Security ), TRANSIENT, hal 83 – 84.

[4] Adhar D , 2014, Pengamanan SQLITE Database Menggunakan Kriptografi Elgamal, Seminar Nasional Informatika 2014, hal 432-437.

[5] S. Hardiyanti S, Musdalifah A, Hendra , 2012, Enkripsi Affine Cipher untuk Steganografi pada Animasi Citra, JIMT Vol. 9 No. 1, hal 89 – 100.