IMPLEMENTASI ALGORITMA ELGAMAL DAN

VIGENERE CIPHER

UNTUK ENKRIPSI DAN DEKRIPSI DATA CITRA DIGITAL

Divananda Zikry Fadilla

*Program Studi Teknik Informatika,Fakultas Teknologi Informasi dan Elektro  
Universitas Teknologi Yogykarta*

*Jl. Ringroad Utara Jombor Sleman Yogyakarta*

*E-mail :* [*divanandazf@gmail.com*](mailto:divanandazf@gmail.com)

## ABSTRAK

*Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak bertanggung jawab. Elgamal adalah salah satu kriptografi yang menggunakan algoritma asimetri. Keamanan dari algoritma Elgamal terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar. Vigenere Cipher adalah salah satu kriptografi yang menggunakan algoritma simetri. Pada proses enkripsi pertama mengambil nilai RGB dari setiap piksel kemudian dihitung dengan nilai P, G, Y dan X yang sebelumnya itu adalah nilai random dari algoritma Elgamal. Hasil pada perhitungan pertama yaitu berupa 2 buah matriks 2x2 yang nantinya matriks pertama akan dideklarasikan menjadi matriks key dan matriks yang kedua akan dihitung kembali menggunakan algoritma Vigenere Cipher. Setelah mendapatkan matriks yang kedua lalu matriks tersebut dihitung dengan nilai ASCII dari setiap karakter Password. Pada tahap ini 2 buah matriks tersebut akan diubah kembali menjadi citra key dan citra enkripsi. Kemudian pada proses dekripsi pertama mengambil nilai RGB dari setiap piksel kemudian dihitung dengan nilai ASCII dari setiap Password. Pada tahap ini proses dekripsi menggunakan algoritma Vigenere Cipher telah selesai, kemudian dilanjut menghitung menggunakan algoritma Elgamal. Selanjutnya citra key akan diambil nilai RGB dari setiap pikselnya kemudian dihitung dan akan menghasilkan nilai RGBX. Pada tahap selanjutnya hasil perhitungan nilai RGB dengan nilai ASCII dari setiap Password akan dihitung dengan nilai P dan X dari algoritma Elgamal dan dikalikan dengan nilai RGBX sebelumnya. Kemudian hasil perhitungan akan menghasilkan 1 buah matriks 2x2 yang akan dideklarasikan menjadi citra dekripsi. Hasil pengujian pada implementasi algoritma Elgamal dan Vigenere Cipher pada proses enkripsi, citra menjadi tidak bisa dibaca. Sedangkan Pada proses dekripsi terdapat beberapa gambar yang hasil kecocokannya tidak sampai 100% dikarenakan perhitungan menggunakan algoritma Elgamal menggunakan bilangan prima dan dipangkatkan dengan bilangan yang cukup besar, sehingga pada saat perhitungan modulo hasilnya ada yang tidak sesuai dengan citra asli.*

Kata kunci : Kriptografi, Enkripsi, Dekripsi, Elgamal, Vigenere Cipher, Data Citra Digital

### 1. PENDAHULUAN

Di era globalisasi seperti saat ini, informasi merupakan hal yang sangat dibutuhkan dalam aspek kehidupan setiap manusia. Salah satu informasi yaitu berupa gambar. Banyak gambar yang sifatnya pribadi yang dimiliki pengguna tersebar luas di jejaring sosial atau dijadikan konsumsi pribadi oleh pihak yang tidak bertanggung jawab. Hal ini bisa terjadi pada saat pengiriman gambar melalui *email* atau pada jejaring sosial.

Untuk itulah, perlu dilakukan sebuah pengamanan pada gambar tersebut. Salah satu contoh pengamanan adalah dilakukannya proses enkripsi dan dekripsi gambar. Proses enkripsi gambar dilakukan untuk membuat gambar tersebut menjadi tidak bisa dipahami, kemudian proses dekripsi gambar dilakukan untuk membuat gambar yang terenkripsi menjadi gambar semula sebelum dienkripsi. Pada saat pengiriman gambar yang sudah terenkripsi melalui *email* atau pada jejaring sosial maka pihak ke 3 tidak memahami arti dari gambar tersebut.

Penelitian terdahulu oleh Alif & Wahid (2015) yang memaparkan enkripsi dan dekripsi gambar bitmap 8 bit menggunakan algoritma *Rivest Shamir Adleman* (RSA) dan *Vigenere Cipher*. Dalam penelitian tersebut menjelaskan menggabungkan dua metode dalam melakukan enkripsi dan dekripsi citra *digital*. Dalam penelitian tersebut hasil pengujian menunjukkan secara *visual* citra hasil enkripsi sulit untuk dibaca atau dilihat dan hasil pengujian untuk dekripsi tidak mengalami cacat sedikitpun dan berhasil kembali ke bentuk semula.

Dalam melakukan enkripsi dan dekripsi dibutuhkan algoritma yang tepat, algoritma yang akan digunakan dalam penelitian ini adalah algoritma *Elgamal* dan *Vigenere Cipher*. Keamanan algoritma *Elgamal* terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar sedangkan algoritma *Viegenere Cipher* mudah dipahami dan diimplementasikan, sehingga dapat menghasilkan enkripsi data citra *digital* yang sulit dibaca dan dapat didekripsikan ke bentuk semula. Berdasarkan latar belakang tersebut maka algoritma enkripsi dan dekripsi tersebut akan diimplementasikan dalam bentuk perangkat lunak.

### 1.1 Rumusan Masalah

Berdasarkan latar belakang, maka rumusan masalah yang di dapat yaitu sebagai berikut:

1. Bagaimana mengimplementasikan algoritma *Elgamal* dan *Vigenere Cipher* pada data citra *digital.*
2. Bagaimana cara kerja dari algoritma *Elgamal* dan *Vigenere Cipher* sebagai salah satu teknik enkripsi dan dekripsi citra.

### 1.2 Batasan Masalah

Dari uraian latar belakang dan rumusan masalah yang telah dijelaskan diatas, maka penelitian ini memiliki beberapa batasan masalah sebagai berikut:

1. Data masukannya adalah bilangan prima, kunci dan data citra *digital* berekstensi png.
2. Data keluarannya adalah data citra *digital* yang sudah dienkripsi.
3. Metode *Elgamal* dan *Vigenere Cipher* diimplementasikan menggunakan bahasa pemrograman Java.
4. Algoritma yang digunakan pada penelitian ini adalah *Elgamal* dan *Vigenere Cipher*.
5. Pada proses enkripsi pertama menggunakan algoritma *Elgamal* kemudian dilanjut menggunakan algoritma *Vigenere Cipher*.
6. Pada proses dekripsi pertama menggunakan algoritma *Vigenere Cipher* kemudian dilanjut menggunakan algoritma *Elgamal*.
7. Kunci yang digunakan untuk enkripsi dan dekripsi minimal 4 karakter.
8. Laporan berupa informasi proses enkripsi dan dekripsi data citra *digital*.

### 1.3 Tujuan Penelitian

Berdasarkan uraian latar belakang, rumusan masalah dan batasan masalah, maka tujuan penelitian ini yaitu sebagai berikut:

1. Untuk mengimplementasikan algoritma *Elgamal* dan *Vigenere Cipher* sebagai teknik enkripsi dan dekripsi citra dengan menggunakan bahasa pemrograman Java.
2. Untuk mengetahui dan memahami cara kerja teknik enkripsi dan dekripsi citra dengan algoritma *Elgamal* dan *Vigenere Cipher*.

### 1.4 Manfaat Penelitian

Dari uraian tujuan penelitian di atas, maka di dapatkan manfaat penelitian sebagai berikut:

1. Dapat mengenkripsi dan dekripsi data citra *digital* yang berekstensi png.
2. Mengamankan data citra *digital* saat bertukar informasi.

### 2. LANDASAN TEORI

**2.1 Kriptografi**

Ariyus (2006) mendefinisikan bahwa kriptografi berasal dari bahasa yunani, menurut bahasa dibagi menjadi dua kripto dan graphia, kripto berarti *secret* (rahasia) dan graphia berarti *writing* (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancangan algoritma kriptografi disebut kriptografer. Kriptografer mencakup teknik enkripsi dan dekripsi.

1. Enkripsi

Enkripsi merupakan proses mengubah *plaintext* menjadi kode-kode yang tidak dapat dimengerti yang disebut *ciphertext* dengan melalui suatu algoritma.

1. Dekripsi

Dekripsi merupakan proses untuk mengubah *ciphertext* menjadi *plaintext* menggunakan algoritma tertentu yang merupakan pasangan dari algoritma enkripsi.

**2.2 Algoritma Simetri**

Ariyus (2006) dalam bukunya menjelaskan algoritma ini juga sering disebut dengan algoritma klasik, karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsinya. Algoritma ini sudah ada lebih dari 4000 tahun yang lalu. Mengirim pesan dengan menggunakan algoritma ini, penerima pesna harus diberitahu kunci dari pesan tersebut agar bisa mendekripsi pesan yang dikiri. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci, jika kunci tersebut diketahui oleh orang lain maka, orang tersebut bisa melakukan enkripsi dan dekripsi terhadap pesan tersebut. Algoritma yang memakai kunci simetri diantaranya adalah DES, RC2, RC4, RC5, RC6, IDEA, AES, OTP, A5 dan lain sebagainya**.**

**2.3 Algoritma Asimetri**

Ariyus (2006) dalam bukunya menjelaskan algoritma asimetri sering juga disebut dengan algoritma kunci public, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsinya berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian :

1. Kunci umum (*public key*) : Kunci yang boleh semua orang tahu (dipulikasikan).
2. Kunci pribadi (*private key*) : Kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci-kunci tersebut saling berhubungan satu dengan yang lainnya. Dengan kunci public orang dapat mengenkripsi pesan tapi tidak bisa mengdekripsinya, hanya orang yang memiliki kunci pribadi yang dapat mendekripsi pesan tersebut. Algoritma asimetris bisa melakukan pengiriman pesan lebih aman dari pada algoritma simetris.

**2.4 Vigenere Cipher**

Ariyus (2006) mendefinisikan *Vigenere Cipher* adalah metode enkripsi abjad majemuk manual (*polyalphabetical substitution cipher*). Algoritma ini ditemukan oleh diplomat sekaligus kriptolog Perancis, Blaisc de Vigenere, pada abad XVI. Metode ini dipublikasikan pada tahun 1856, dan sekitar dua ratus tahun setelahnya, pada abad XIX. *Vigenere Cipher* digunakan oleh Tentara Konfederasi pada Perang Sipil Amerika. Pada dasarnya *Vigenere Cipher* menggunakan teknik-teknik yang sama dengan *Caesar Cipher*. Bedanya dalam *Vigenere Cipher* setiap huruf dalam *plaintext* dapat dienkripsikan menggunakan kunci yang berbeda. Huruf pertama pada *plaintext* dienkripsikan dengan kunci berupa huruf pertama dari kata kunci, dan seterusnya.

Pengembangan dari metode *Vigenere Cipher* untuk penyandian citra dilakukan dengan menggunakan formula *Vigenere Cipher* dengan menggunakan nilai basis modulo 256 sesuai dengan intensitas warna pada citra. Kunci-kunci tersebut disebut dengan *Vigenere Table*. Dalam implementasinya tabel tersebut dikembangkan dengna nilai *plaintext* dari 0 sampai dengan 255. Rumus enkripsi yang digunakan untuk menghitung nilai cipher image tiap pixel adalah sebagai berikut :

Dengan : a : Intensitas citra pixel ke-i,j dari citra asli

Ki : Kunci ke-i

E : Citra enkripsi

Sedangkan rumus yang digunakan untuk mendapatkan citra yang sudah dienkripsi (dekripsi) adalah sebagai berikut :

Dengan : a : Intensitas citra pixel ke-i,j dari citra yang sudah terenkripsi

Ki : Kunci ke-i

D : Citra dekripsi

**2.5 Elgamal**

Ariyus (2006) dalam bukunya menjelaskan Elgamaladalah suatu *public-key cryptosystem* yang dibuat pada tahun 1985. Algoritma Elgamal digunakan untuk melakukan enkripsi. Keamanan dari Elgamalterletak pada susahnya dari perhitungan logaritma yang terpisah pada GF (p) ketika p merupakan bilangan prima yang besar. Faktorisasi utama dari logaritma yang terpisah diperlukan dianjurkan untuk diimplementasikan pada RSA dan Elgamal *cryptosystem*. Teknik perhitungan dasar untuk enkripsi menggunakan algoritma *El Gamal* dengan dua kunci *cryptosystem* adalah sebagai berikut :

*Public key* :

*p* (bilangan prima)

*g, x < p* (dua bilangan acak)

(*public key*)

*Private Key* :

*x < p*

Enkripsi :

*k* : bilangan acak dimana *k < p*

Dekripsi :

**2.6 Citra Digital**

Munir (2004) mendefinisikan sebuah citra *digital* adalah kumpulan piksel-piksel yang disusun dalam larik dua dimensi yang dapat diobservasi oleh sistem visual manusia. Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*continue*) dari intesitas cahaya pada bidang dwimitra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut. Pantulan cahaya ini ditangkap oleh alat-alat optik, misalnya mata manusia, kamera digital, dan sebagainya, sehingga banyak objek citra tersebut terekam. Agar dapat diolah dengan komputer digital, suatu citra harus direpresentasikan secara numerik dengan nilai-nilai diskrit. Representasi citra dari fungsi *continue* menjadi nilai-nilai diskrit disebut pencitraan (*imaging*) atau digitalisasi. Citra yang dihasilkan inilah yang disebut citra *digital* yang dinyatakan sebagai kumpulan piksel dalam matriks dua dimensi.

### 3. METODOLOGI PENELITIAN

## 3.1 Metode Penelitian

Metode penelitian yang digunakan pada penelitian ini termasuk di dalam jenis penelitian terapan. Penelitian terapan ini bertujuan untuk merancang dan membangun sebuah aplikasi sebagai enkripsi dan dekripsi data citra digital.

### 3.2 Pengumpulan data

Pengumpulan data adalah suatu metode dan prosedur yang digunakan untuk mendapatkan suatu informasi tentang algoritma enkripsi data citra digital. Tahap pengumpulan data ini terdapat beberapa hal yang harus dilakukan, antara lain :

1. Studi Pustaka

Metode pengumpulan data dengan cara membaca dan mempelajari referensi dan buku-buku, jurnal dan internet sebagai referensi penulis dalam menyusun penelitian yang berkaitan dengan permasalahan yang diteliti.

1. Desain

Representasi dari :

1. Struktur data
2. Struktur program
3. Karakteristik *interface*
4. Detail prosedur
5. Implementasi

Implementasi sistem merupakan sistem yang baru dikembangkan tersebut siap dioperasikan sesuai apa yang diharapkan. Tujuan dari tahap implementasi ini merupakan transformasi konsep rancangan menjadi wujud sistem yang utuh dan dapat digunakan.

1. Pengujian (*Testing*)

Setelah sistem selesai direalisasikan melalui tahap implementasi, sistem perlu dilakukan pengujian (*testing*). Tahap ini dilakukan untuk mengetahui apakah sistem yang dibuat telah memenuhi fungsi-fungsi sesuai dengan analisis sistem. Pengujian juga dilakukan untuk mengetahui ada tidaknya kesalahan atau *error* dari sistem yang telah dibuat. Jika *error* ditemukan pada sistem, maka tahap akan diulang dari analisis sistem hingga pengkodean.

**4. HASIL DAN PEMBAHASAN**

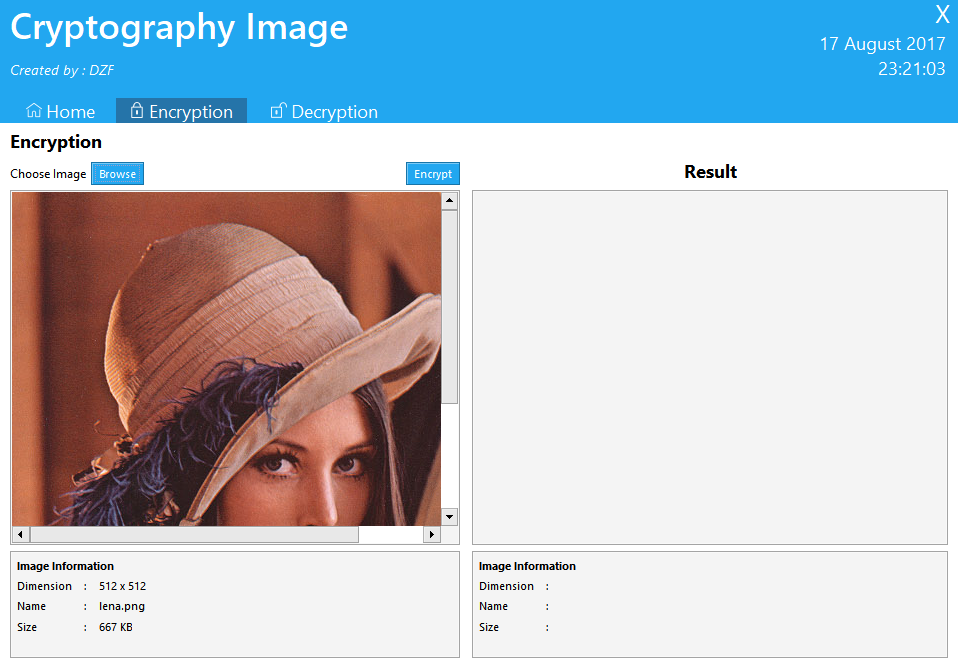
**4.1 Analisa Kerja Sistem**

Adapun proses dan alur kerja sistem secara umum adalah sebagai berikut :

1. Saat menggunakan sistem, pengguna akan melakukan *input* data berupa citra yang akan dienkripsi.
2. Pada proses sebelum melakukan enkripsi, pengguna diharuskan membuat password, *public key* dan *private key* yang nantinya akan digunakan dalam perhitungan enkripsi dan dekripsi.
3. Citra selanjutnya akan dilakukan proses enkripsi menggunakan algoritma Elgamal, kemudian hasil dari perhitungan menggunakan algoritma Elgamal dihitung lagi menggunakan algoritma Vigenere Cipher.
4. Hasil *output* yang akan diterima oleh pengguna berupa citra yang sudah terenkripsi dan citra *key* yang nantinya digunakan untuk proses dekripsi citra.
5. Proses dekripsi membutuhkan *input* citra yang sudah terenkripsi, citra *key* dan *password.*
6. Citra selanjutnya akan dilakukan proses dekripsi menggunakan algoritma Vigenere Cipher terlebih dahulu, kemudian hasil dari perhitungan tersebut dihitung lagi menggunakan algoritma Elgamal.
7. Hasil *output* yang akan diterima oleh pengguna berupa citra yang sudah didekripsi atau citra awal sebelum dilakukan enkripsi.

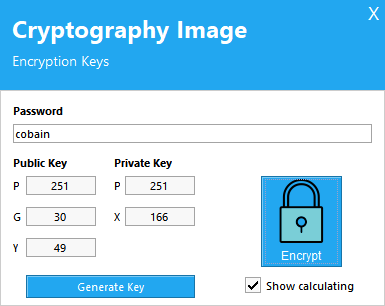
**4.2 Enkripsi**

Proses enkripsi citra pertama dihitung menggunakan algoritma Elgamal dan kemudian hasil dari perhitungan dihitung kembali menggunakan algoritma Vigenere Cipher. Gambar yang akan dienkripsi akan dipilih menggunakan tombol *Browse*. Setelah gambar dipilih maka aplikasi akan menampilkan data gambar tersebut berupa nama, ukuran piksel dan ukuran memori dari gambar tersebut. Kemudian tombol *encrypt* digunakan untuk melanjutkan proses enkripsi. Setelah menekan tombol *encrypt*, aplikasi akan meminta *user* untuk memasukkan *password, public key* dan *private key*. Jika proses enkripsi sudah dilakukan maka hasil dari enkripsi berupa gambar yang berekstensi key dan gambar yang sudah terenkripsi akan ditampilkan pada form *result* berupa gambar yang sudah terenkripsi, nama gambar, ukuran piksel dan ukuran memori dari gambar yang sudah terenkripsi*.* Tampilan halaman *encryption* dapat dilihat pada gambar 1.



*Gambar 1: Form encryption sebelum perhitungan*

Form *encryption keys* merupakan halaman yang digunakan *user* untuk memasukkan *password*, *public key* dan *private key* yang nantinya akan digunakan untuk perhitungan enkripsi gambar. Pada halaman *encryption keys* terdapat menu *show calculating* yang nantinya akan digunakan untuk menampilkan perhitungan enkripsi. Tampilan halaman *encryption keys* dapat dilihat pada gambar 2.



*Gambar 2: Form encryption keys*

Pada halaman *encryption keys* terdapat *password* yang nantinya setiap karakter akan diubah menjadi nilai desimal ASCII. Nilai setiap karakter tersebut akan digunakan dalam perhitungan enkripsi menggunakan algoritma Vigenere Cipher. Kemudian *public key* dan *private key* merupakan kunci yang nilainya *random*. Untuk mendapatkan nilai *random*, sistem hanya memanggil fungsi Math.rand() yang sudah tersedia pada bahasa pemrograman Java. Nilai P menggunakan nilai tetap yaitu 251 dikarenakan nilai P merupakan bilangan prima, sedangkan bilangan prima yang mendekati dengan 255 adalah 251. Kemudian untuk nilai Y didapat dari perhitungan . Kemudian nilai P, G, Y dan X tersebut akan digunakan dalam perhitungan enkripsi menggunakan algoritma Elgamal. Jika *password, public key* dan *private key* sudah terisi maka bisa melanjutkan ke tahap selanjutnya dengan menekan tombol *Encrypt*. Setelah menekan tombol tersebut maka perhitungan pun dimulai. Perhitungan pertama mengambil intensitas citra RGB pada setiap piksel, kemudian piksel tersebut dihitung menggunakan algoritma Elgamal. Pada tahap ini perhitungan menggunakan algoritma Elgamal akan menghasilkan 2 buah matriks 2x2. Matriks yang pertama akan dideklarasikan menjadi gambar *key* dan matriks yang kedua akan dihitung kembali menggunakan algoritma Vigenere Cipher. Perhitungan menggunakan algoritma Elgamal adalah sebagai berikut :

Iterasi piksel ke 0,0

Pada setiap iterasi sistem akan membuat nilai random K.

\*nilai random < P

Kemudian mengambil nilai RGB pada citra.

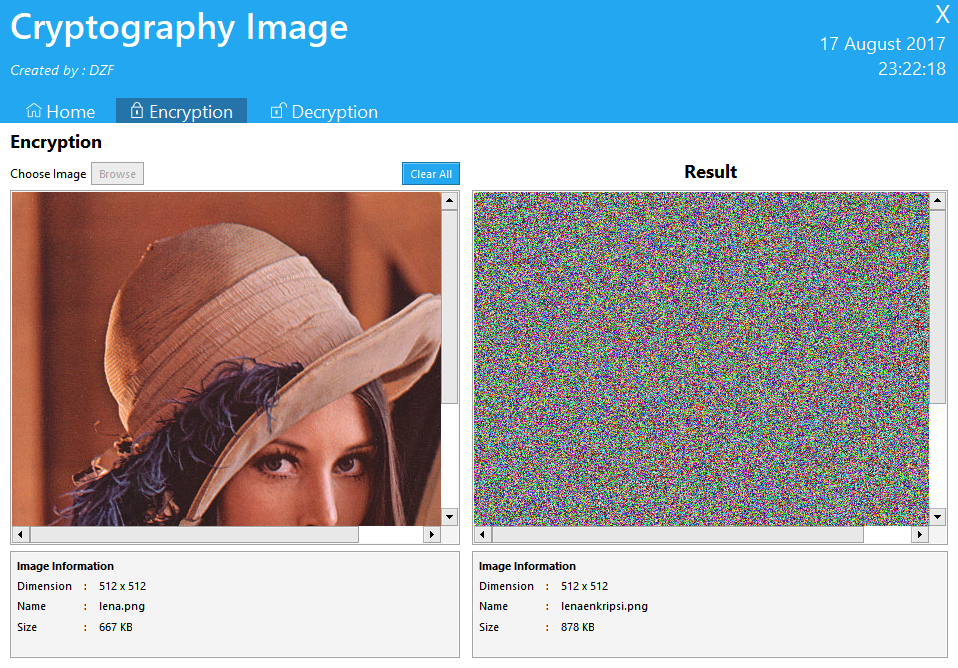
Pada saat pengambilan nilai RGB apabila ditemukan yang nilainya diatas 251 maka nilai tersebut akan diubah menjadi 250. Hal ini dikarenakan mod yang digunakan adalah 251. Kemudian pada iterasi 0,0 nilai Alpha akan diubah menjadi nilai P dan pada iterasi 0,1 nilai Alpha akan diubah menjadi nilai X. Kemudian menghitung matriks pertama menggunakan rumus . Hasil perhitungannya adalah sebagai berikut :

Kemudian menghitung matriks kedua menggunakan rumus . Hasil perhitungannya adalah sebagai berikut :

Selanjutnya adalah tahap perhitungan menggunakan algoritma Vigenere Cipher. Matriks enkripsi yang sebelumnya sudah dihitung menggunakan algoritma Elgamal kemudian dihitung kembali dengan rumus Vigenere Cipher. *Password* yang sebelumnya diinputkan akan digunakan dalam perhitungan Vigenere Cipher. Setiap karakter pada *password* akan diubah menjadi nilai ASCII. Contoh *password* pada gambar 2 adalah ‘cobain’ maka nilai ASCII dari c=99, o=111, b=98, a=97, i=105 dan n=110. Pada iterasi 0,0 maka akan menggunakan c=99, kemudian iterasi 0,1 akan menggunakan o=111 dan seterusnya hingga pada iterasi 0,5 akan menggunakan n=110. Jika sudah mencapai karakter terakhir dari *password* maka akan menggunakan karakter pertama kembali. Maka iterasi 0,6 akan menggunakan c=99. Perhitungan menggunakan algoritma Vigenere Cipher adalah sebagai berikut :

Menentukan nilai ASCII

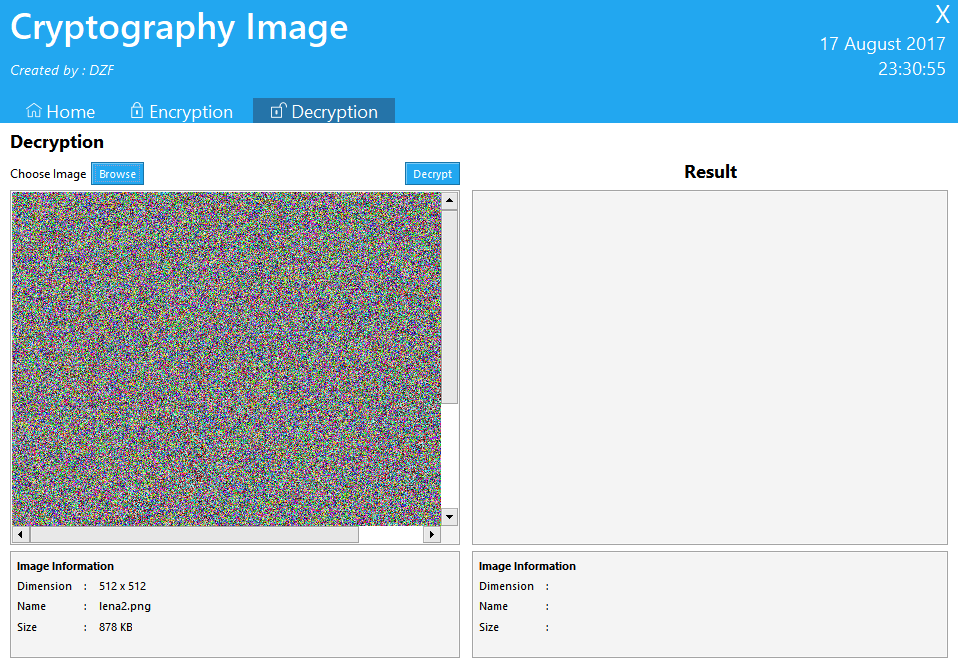
Kemudian melanjutkan perhitungan pada iterasi selanjutnya hingga sampai pada iterasi terakhir. Pada tahap ini sudah didapatkan 2 buah matriks, yaitu matriks key dan matriks vigenere yang kemudian ke-2 matriks tersebut akan diubah menjadi gambar yang berekstensi png dan akan disimpan pada tempat penyimpanan yang ditentukan. Kemudian hasil gambar yang sudah terenkripsi akan ditampilkan pada halaman *encryption*. Tampilan halaman *encryption* setelah melakukan perhitungan dapat dilihat pada gambar 3.



*Gambar 3: Form encryption setelah perhitungan selesai*

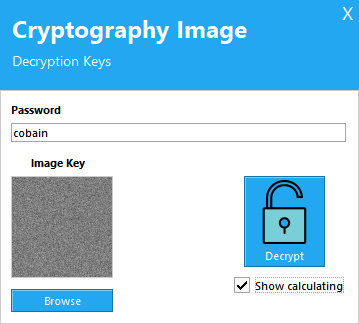
**4.3 Dekripsi**

Proses dekripsi citra pertama dihitung menggunakan algoritma Vigenere Cipher kemudian hasil perhitungannya dihitung kembali menggunakan algoritma Elgamal. Gambar yang akan didekripsi akan dipilih menggunakan tombol *Browse*. Setelah gambar dipilih maka aplikasi akan menampilkan data gambar tersebut berupa nama ,ukuran piksel dan ukuran memori dari gambar tersebut. Kemudian tombol *decrypt* digunakan untuk melanjutkan proses dekripsi. Setelah menekan tombol *decrypt*, aplikasi akan meminta *user* untuk memasukkan *password* dan *image key*. Jika proses dekripsi udah dilakukan maka hasil dari dekripsi akan ditampilkan pada form *result* berupa gambar yang sudah didekripsi, nama gambar dan ukuran gambar yang sudah terdekripsi. Tampilan halaman *decryption* dapat dilihat pada gambar 4.



*Gambar 4: Form decryption sebelum melakukan perhitungan*

Pada halaman *decryption keys* terdapat *password* yang nantinya setiap karakter akan diubah menjadi nilai desimal ASCII. Nilai setiap karakter tersebut akan digunakan dalam perhitungan dekripsi menggunakan algoritma Vigenere Cipher. Kemudian *Image Key* adalah matriks key yang didapatkan dari perhitungan menggunakan algoritma enkripsi Elgamal. Untuk *input image key* diharuskan mempunyai ukuran piksel yang sama dengan gambar yang akan didekripsi. *Image Key* akan digunakan dalam perhitungan dekripsi menggunakan algoritma Elgamal. Tampilan halaman *decryption keys* dapat dilihat pada gambar 5.



*Gambar 5: Form decryption keys*

*Password* yang sebelumnya diinputkan akan digunakan dalam perhitungan Vigenere Cipher. Setiap karakter pada *password* akan diubah menjadi nilai ASCII. Contoh *password* pada gambar 5 adalah ‘cobain’ maka nilai ASCII dari c=99, o=111, b=98, a=97, i=105 dan n=110. Pada iterasi 0,0 maka akan menggunakan c=99, kemudian iterasi 0,1 akan menggunakan o=111 dan seterusnya hingga pada iterasi 0,5 akan menggunakan n=110. Jika sudah mencapai karakter terakhir dari *password* maka akan menggunakan karakter pertama kembali. Maka iterasi 0,6 akan menggunakan c=99. Pada perhitungan menggunakan algoritma Vigenere Cipher akan menghasilkan 1 buah matriks 2x2. Perhitungan menggunakan algoritma Vigenere Cipher adalah sebagai berikut :

Iterasi 0,0

Menentukan nilai ASCII .

Kemudian mengambil nilai RGB pada citra

Kemudian menghitung menggunakan rumus dekripsi Vigenere Cipher. Hasil perhitungannya adalah sebagai berikut :

Selanjutnya adalah tahap perhitungan menggunakan algoritma Elgamal. I*mage key* yang sebelumnya sudah diinputkan akan diambil intensitas citra RGB pada setiap piksel nya. Dalam melakukan dekripsi menggunakan algoritma Elgamal membutuhkan nilai P dan X. Pada tahap enkripsi nilai P dan X sudah disimpan di dalam gambar yang terenkripsi dengan nilai Alpha pada piksel 0,0 dan 0,1. Perhitungan dekripsi menggunakan algoritma Elgamal adalah sebagai berikut :

\*mengambil nilai Alpha pada piksel 0,0

\* mengambil nilai Alpha pada piksel 0,1

Jika nilai P dan X sudah diambil maka nilai Alpha pada 0,0 dan 0,1 akan diubah kembali menjadi 255. Lalu mengambil nilai RGB pada *Image Key.*

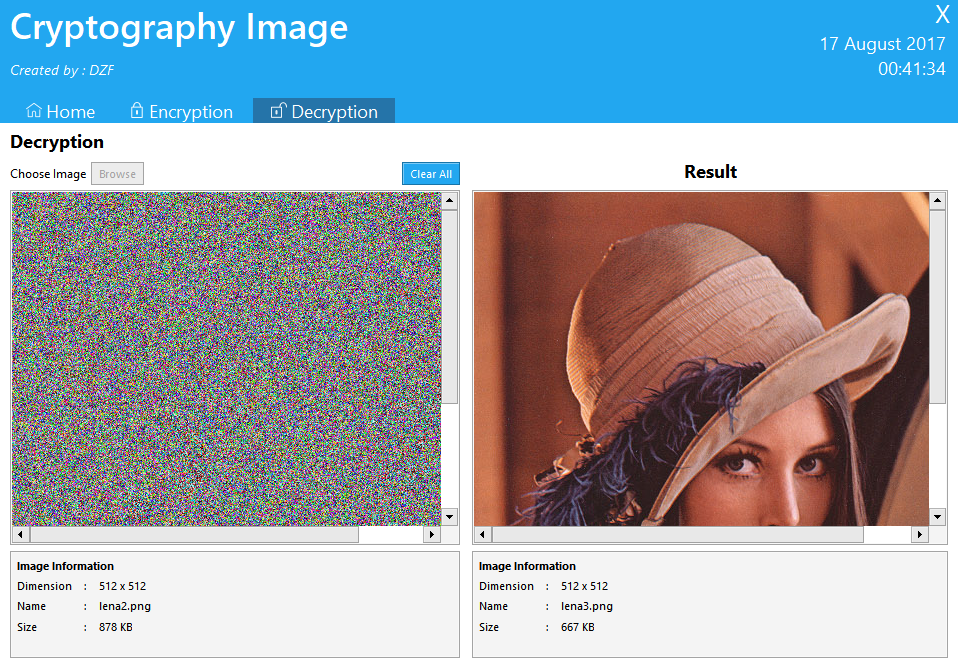
Kemudian menghitung *Image Key* dengan rumus sebagai berikut :

Maka hasil perhitungannya adalah sebagai berikut :

Setelah mendapatkan RGBX kemudian menghitung RGBX dan RGBVigenere dengan rumus sebagai berikut :

Maka hasil perhitungannya adalah sebagai berikut :

Kemudian melanjutkan perhitungan pada iterasi selanjutnya hingga sampai pada iterasi terakhir. Pada tahap ini sudah didapatkan 1 buah matriks yaitu matrik dekripsi elgamal yang kemudian matriks tersebut akan diubah menjadi gambar yang berekstensi png dan akan disimpan pada tempat penyimpanan yang ditentukan. Kemudian hasil gambar yang sudah terdekripsi akan ditampilkan pada halaman *decryption*. Tampilan halaman *decryption* setelah melakukan perhitungan dapat dilihat pada gambar 6.

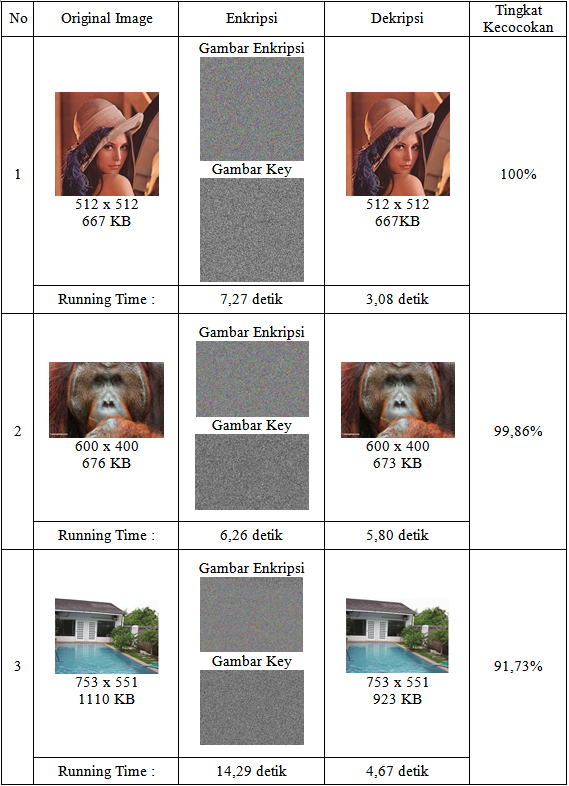


*Gambar 6: Form decryption setelah perhitungan*

**4.4 Hasil Pengujian**

Setelah sistem selesai dibuat, dilakukan 3 pengujian terhadap sistem ini. Pengujian dilakukan untuk melihat hasil enkripsi, perbedaan waktu terhadap ukuran citra dan pengujian untuk melihat apakah citra hasil dekripsi sama dengan citra *original.*

*Tabel 1: Hasil pengujian*

****

Berdasarkan pengujian yang dilakukan dapat disimpulkan bahwa waktu proses enkripsi lebih lama dibandingkan proses dekripsi. Hal ini dikarenakan pada saat melakukan proses enkripsi melakukan pembentukan 2 buah matriks dan menghasilkan 2 buah gambar yaitu gambar enkripsi dan gambar *key*. Ukuran piksel citra juga mempengaruhi waktu proses enkripsi dan dekripsi. Semakin tinggi ukuran piksel citra maka proses nya semakin lama. Sedangkan dari hasil tingkat kecocokan antara gambar *original* dan gambar dekripsi pada pengujian gambar 1 memiliki tingkat kecocokan 100% sedangkan pada gambar 2 dan 3 memiliki tingkat kecocokan dibawah 100%. Hal tersebut dikarenakan pada gambar 2 dan 3 terdapat nilai RGB pada piksel tertentu yang nilainya lebih dari 251. Pada proses enkripsi, jika ditemukan nilai RGB yang lebih dari 251 maka nilai RGB tersebut akan diubah menjadi 250. Contoh pada gambar 3 pada piksel 0,0 bernilai 255 maka piksel tersebut diubah menjadi 250. Semakin banyak nilai RGB yang diatas 251 maka tingkat kecocokannya semakin menurun.

**5. PENUTUP**

**5.1. Kesimpulan**

Berdasarkan hasil analisis dan penelitian yang dilakukan, maka didapat kesimpulan sebagai berikut:

1. Aplikasi dapat melakukan proses enkripsi dan dekripsi gambar dengan perhitungan yang sesuai dengan algoritma yang digunakan.
2. Algoritma Vigenere Cipher dapat melakukan enkripsi dan dekripsi gambar dengan sempurna.
3. Algoritma Elgamal dapat melakukan enkripsi dan dekripsi gambar, tetapi hasil dekripsi, pixel tidak 100% kembali seperti pixel asli dikarenakan pada algoritma Elgamal menggunakan modulo bilangan prima.
4. Algoritma Elgamal dan Vigenere Cipher dapat melakukan enkripsi dan dekripsi gambar, tetapi hasil dekripsi, pixel tidak 100% kembali seperti pixel asli dikarenakan pada algoritma Elgamal menggunakan modulo bilangan prima.
5. Jika ada kesalahan ketika memasukan data.

**5.2. Saran**

Berdasarkan kesimpulan diatas, maka terdapat beberapa saran guna membangun pembaca dari tulisan ini, yaitu sebagai berikut:

1. Perlu adanya tambahan algoritma dalam penyelesaian enkripsi dan dekripsi gambar.
2. Penambahan ekstensi gambar yang akan dienkripsi dan dekripsi.

**Daftar pustaka**

[1] Agung, G., 2016, *Belajar Java, Database dan NetBeans dari Nol,* Yogyakarta: Jubilee Enterprise.

[2] Alif, Andro., dan Wahid, Achmad. 2015, *Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) dan Vigenere Cipher Pada Gambar Bitmap 8 Bit*, Jurnal, Teknik Informatika, Universitas Dian Nuswantoro, Semarang.

[3] Anna, Theresia., Pakereng, Ineke., dan Richard, Yos. 2009, *Implementasi Algoritma Chaos-Based Feedback Stream Cipher pada Enkripsi-Dekripsi Data Citra Digital*, Jurnal, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.

[4] Aprianto, Yoga., Kurniawan, Rico., dan Angreni, Reni. 2014, *Rancang Bangun Aplikasi Enkripsi dan Dekripsi Citra Digital Menggunakan Algoritma Rijndael Berbasis Java SE*, Jurnal, Teknik Informatika, STMIK GI MDP, Palembang.

[5] Ariyus, D., 2006, *Kriptografi Keamanan Data dan Komunikasi*, Yogyakarta: Graha Ilmu.

[6] Munir, R., 2004, *Pengolahan Citra Dengan Pendekatan Algoritmik.* Informatika, Bandung: Informatika Publishing

[7] Rachmat, Antonius dan Wikan, Aditya. 2016, *Konsep dan Implementasi Pemrograman GUI*, Yogyakarta: ANDI.

[8] Whitten, Jeffrey., Bentley, Lonnie., dan Dittman, Kevin. 2004, *System Analysis and Design Methods*, Boston: McGraw-Hill Companies.