**Journal of Informatics, Electrical and Electronics Engineering**
ISSN 2807-9507 (Media Online)
Vol 1, No 2, Desember 2021
Hal 67-74
https://djournals.com/jieee

# Implementasi Kriptografi *Hybrid* Algoritma *Elgamal* Dan *Double Playfair Cipher* Dalam Pengamanan File Jpeg Berbasis Dekstop

**Irwansyah Putra Sinaga**

Program Studi Teknik Informatika Universitas Budi Darma, Medan, Indonesia

Email : insyah1067@gmail.com

**Abstrak-**Citra digital merupakan representatif dari citra yang diambil oleh mesin dengan bentuk pendekatan berdasarkan sampling dan kuantisasi. Sampling menyatakan besarnya kotak-kotak yang disusun dalam baris dan kolom. Dengan kata lain, sampling pada citra menyatakan besar kecilnya ukuran *pixel* (titik) pada citra, dan kuantisasi menyatakan besarnya nilai tingkat kecerahan yang dinyatakan dalam nilai tingkat keabuan (*grayscale*) sesuai dengan jurnlah bit biner yang digunakan oleh mesin, dengan kata lain kuantisasi pada citra menyatakan jumlah warna yang ada pada citra. Sangatlah penting dalam mengamankan citra digital dari pihak yang tidak memiliki hak akses menjadi sangat penting. Bila informasi penting dalam bentuk citra digital tersebut jatuh ke tangan orang yang salah, maka akan menyebabkan hal yang tidak diinginkan, contohnya manipulasi gambar dengan bentuk yang negatif dan dapat merugikan pemilik gambar. Dalam menyelesaikan masalah tersebut, penulis menggunakan metode ElGamal yang digunakan untuk menjaga keamanan data tersebut dengan cara menghitung logaritma diskrit pada grup bilangan bulat prima yang di dalamnya dilakukan operasi perkalian serta menggabungkannya dengan metode *Double Playfair Cipher* untuk melakukan penyandian enkripsi citra dan Algoritma ElGamal untuk mengenkripsi kunci dari *Double Playfair Cipher*. Citra pertama kali dienkripsi menggunakan Algoritma *Double Playfair Cipher*, kemudian kunci *Double Playfair* tersebut dienkripsi dengan menggunakan Algoritma ElGamal. Hasil dari pengujian aplikasi yang dirancang adalah terbentuk nya kunci publik dan kunci privat yang dilakukan dalam mengenkripsi dan mendekripsi suatu *file* citra sehingga pertukaran informasi yang berbentuk citra digital dapat dilakukan dengan aman.

**Kata Kunci:** Citra Digital, ElGamal, Double Playfair Cipher

**Abstract-**Digital image is a representative of the image taken by the machine with a form of approach based on sampling and quantization. Sampling states the size of the boxes arranged in rows and columns. In other words, sampling on the image states the size of the pixels (dots) in the image, and quantization states the value of the brightness level expressed in grayscale values according to the number of binary bits used by the machine, in other words quantization in the image represents the number of colors in the image. It is very important in securing digital images from parties who do not have access rights is very important. If important information in the form of digital images falls into the wrong hands, it will cause unwanted things, for example image manipulation in a negative form and can harm the owner of the image. In solving this problem, the author uses the ElGamal method which is used to maintain the security of the data by calculating the discrete logarithm of a group of prime integers in which the multiplication operation is carried out and combining it with the Double Playfair Cipher method to encode the image encryption and the ElGamal Algorithm to encrypt the key. from Double Playfair Cipher. The image is first encrypted using the Double Playfair Cipher Algorithm, then the Double Playfair key is encrypted using the ElGamal Algorithm. The result of testing the designed application is the formation of a public key and a private key which is carried out in encrypting and decrypting an image file so that the exchange of information in the form of digital images can be carried out safely.

**Keywords:** Digital Image, ElGamal, Double Playfair Cipher

## 1. PENDAHULUAN

Citra digital merupakan representatif dari citra yang diambil oleh mesin dengan bentuk pendekatan berdasarkan sampling dan kuantisasi. Sampling menyatakan besarnya kotak-kotak yang disusun dalam baris dan kolom. Dengan kata lain, sampling pada citra menyatakan besar kecilnya ukuran *pixel* (titik) pada citra, dan kuantisasi menyatakan besarnya nilai tingkat kecerahan yang dinyatakan dalam nilai tingkat keabuan (*grayscale*) sesuai dengan jurnlah bit biner yang digunakan oleh mesin [1].

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan data yang berhubungan dengan aspek keamanan informasi. Hal ini bertujuan agar sebuah data yang disampaikan hanya dimengerti oleh orang yang berhak untuk mengetahuinya dan tidak ada pihak lain yang terlibat. Salah satu contoh dari ilmu kriptografi adalah algoritma kunci simetris dan kunci asimetris. Algoritma kunci simetris adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma kunci asimetris adalah algoritma yang memiliki dua buah kunci yaitu kunci publik sebagai media pengenkripsi dan kunci privat sebagai media pendekripsiannya [2].

Dengan menggunakan metode algoritma ElGamal dan Algoritma *Double Playfair Cipher* sesuai untuk mengamankan citra berbentuk file Jpeg. pada tahap enkripsi, hasil enkripsi dengan menggunakan metode *Playfair Cipher* lebih baik dari hasil enkripsi metode ElGamal dikarenakan secara kasat mata, hasil citra yang dienkripsi dengan metode ElGamal masih menunjukkan corak/pola yang lebih jelas/menyerupai citra sebelum dienkripsi dibandingkan dengan citra yang dienkripsi dengan metode Playfair Ciper. Sedangkan pada tahap dekripsi, hasil dekripsi dengan menggunakan metode ElGamal lebih baik dibandingkan metode Playfair Cipher dikarenakan metode ElGamal memiliki hasil citra dekripsi yang lebih menyerupai

citra aslinya. Rata-rata waktu yang diperlukan untuk melakukan proses enkripsi dan dekripsi pada metode Playfair Cipher adalah 2.743 detik dan 3.841, sedangkan pada metode ElGamal membutuhkan waktu rata-rata sekitar 2.327 detik dan 1.937 detik. Dan Penyandian Data Teks Dengan Algoritma Elgamal Dan Algoritma Kompresi Data Dengan Algoritma *Elias Gamma Code*[3]. Hasil penelitian menunjukkan bahwa metode ElGamal dapat menjaga keamanan, kerahasiaan data, dan mengembalikan *file* teks setelah dekripsi seperti *file* awal sebelum proses enkripsi. *File* teks yang sudah di enkripsi menjadi cipherteks memiliki karakter yang lebih banyak atau panjang dibandingkan dengan *file* teks sebelum dilakukan proses enkripsi.

# 2. METODOLOGI PENELITIAN

## 2.1 Kriptografi

Kriptografi merupakan metode untuk mengamankan data, baik itu data teks maupun data gambar. Metode ini dilakukan dengan penyandian atau pengacakan data asli, sehingga pihak lain yang tidak mempunyai hak akses atas data tersebut tidak dapat memperoleh informasi yang ada didalamnya. Secara umum ada dua tipe algoritma kriptografi berdasarkan kuncinya yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris adalah algoritma yang memiliki kunci enkripsi dan dekripsi yang sama,sedangkan untuk algoritma asimetris terdiri atas 2 buah kunci yaitu kunci publik untuk melakukan enkripsi sedangkan kunci pribadi untuk melakukan dekripsi.

## 2.2 Algoritma ElGamal

Algoritma ElGamal yang termasuk algoritma simetris ini diusulkan oleh Taher ElGamal pada tahun 1984.Keamanan dari algoritma ini didasarkan pada kesulitan memecahkan masalah logaritma yang terdapat dalam grup. Logaritma ini sendiri disebut logaritma diskrit karena nilainya berhingga dan bergantung pada bilangan prima yang digunakan.

Algoritma ElGamal mempunyai kunci publik berupa tiga pasang bilangan dan kunci rahasia berupa satu bilangan.Algoritma ini mempunyai kerugian pada cipherteksnya yang mempunyai panjang dua kali lipat dari plainteksnya.Akan tetapi, algoritma ini mempunyai kelebihan pada enkripsi. Untuk plainteks yang sama, algoritma ini memberikan cipherteks yang berbeda setiap kali plainteks dienkripsi. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan *cipher blok*, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan.

## 2.3 Algoritma *Double Playfair Cipher*

*Double playfair* atau yang biasa disebut juga dengan *two-square cipher* muncul sebagai modifikasi dan pengembangan lebih lanjut.*Double playfair cipher* diklaim sebagai metode enkripsi yang lebih baik dibandingkan dengan *playfair*.Double Playfair adalah perpanjangan dari playfair, sebagai turunan dari *playfair cipher*, *double playfair cipher* juga dianggap sebagai algoritma kriptografi klasik. Dalam *double playfair cipher*, cara penempatan kunci dalam persegi huruf masih sama dengan *playfair* biasa. Bedanya adalah, ada dua persegi yang diletakkan bersampingan.Berarti, ada sebuah kunci yang dibagi menjadi dua subkunci. Seperti Playfair, Double Playfair cipher menggunakan kotak 5x5. berikut contoh dari persegi untuk dekripsi enkripsi *double playfair cipher*.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| P | L | A | Y | F | | T | W | O | S | Q |
| I | R | B | C | D | | U | A | R | E | B |
| E | G | H | K | M | | C | D | F | G | H |
| N | O | Q | S | T | | I | K | L | M | N |
| U | V | W | X | Z | | P | V | X | Y | Z |

**Gambar 1.**Contoh Persegi Untuk Dekripsi Enkripsi *Double Playfair*

## 2.4 Bahasa Pemrograman *Visual Basic 2008*

*Microsoft Visual Basic 2008* merupakan bagian dari kelompok bahasa pemrograman Visual Studio 2008 yang dikembangkan oleh *Microsoft.Visual Studio 2008* terdiri dari beberapa bahasa pemrograman di antaranya adalah *Microsoft Visual Basic 2008, Microsoft C# 2008, Microsoft Visual C++ 2008, Microsoft Visual J#,* dan *Visual Web Developer 2008*. *Microsoft Visual Basic 2008* setara dengan *Visual Basic 9.0* yang memiliki kelebihan – kelebihan, yaitu *support* dengan bahasa *Query Language – Integrated Query* (LINQ) dan *support* dengan database *Microsoft SQL Server Compact 3.5*. Selain itu, kelebihan lain adalah memiliki *Object Relational Designer* (O/R *Desaigner*) untuk membantu mengedit LINQ ke SQL yang akan dihubungkan dengan database dan fitur lain, seperti WPF (*Windows Presentation Foundation*) dan WCF (*Windows Communication Foundation*). Semual hal yang barutersebut

ISSN 2807-9507 (Media Online)
Vol 1, No 2, Desember 2021
Hal 67-74
https://djournals.com/jieee

atas menambah kelengkapan aplikasi *Microsoft Visual Basic 2008*[3].

# 3. HASIL DAN PEMBAHASAN

Perkembangan dalam bidang teknologi seperti saat ini telah memungkinkan setiap orang untuk saling melakukan pertukaran informasi tanpa ada batasan jarak dan waktu. Tidak tertutup kemungkinan adanya kebocoran data pada saat proses pertukaran informasi yang dilakukan sehingga pengirim informasi merasa takut dan memerlukan adanya keamanan dalam pertukaran informasi tersebut. Untuk dapat mengurangi ancaman yang dapat terjadi dalam pertukaran informasi yang bersifat rahasia dalam sebuah proses komunikasi data dapat dilakukan dengan cara melakukan pengkodean terhadap informasi yang akan disimpan atau dikirim secara cepat dan akurat.

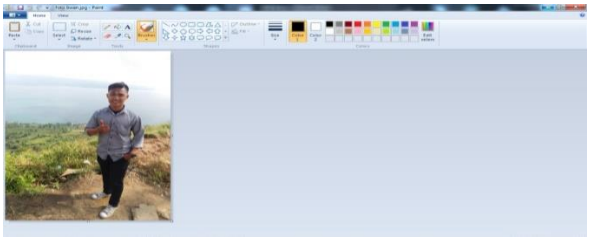
Berdasarkan masalah yang telah diuraikan di atas, peneliti akan menggunakan algoritma Elgamal dengan *Double Playfair Chiper* dalam mengenkripsi dan mendekripsi suatu *file* citra dengan ekstensi (*.jpeg) karena menurut penelitian sebelumnya dengan menggunakan kedua algoritma tersebut diharapkan akan memiliki kelebihan dalam melakukan penyandian pada *file* citra dengan ekstensi (*.jpeg).

## 3.1 Contoh Kasus

Contoh kasus yang diambil untuk penelitian ini adalah misalkan pada citra yang akan dienkripsi adalah citra yang berukuran 1024 x 768 piksel. Tampilan dari citra yang akan diuji dapat dilihat pada Gambar 3.1 sebagai berikut.

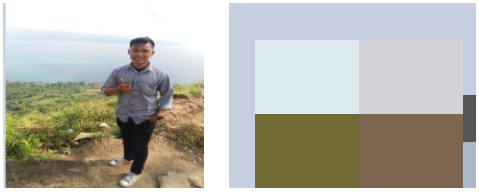
**Gambar 1.** Citra yang akan Diuji

1. Merubah Gambar Menjadi Data Matriks Menggunakan Matlab.
   Untuk merubah gambar menjadi data matriks menggunakan Matlab dengan menerapkan metode Elgamal dan *Double Playfair Chiper* di mana citra di atas diperkecil menjadi resolusi 2x2 untuk mempermudah proses analisa terhadap citra yang memiliki *noise* dengan menggunakan *paint*.



**Gambar 2.** Memperkecil Piksel 2x2

Hasil citra yang telah diperkecil menjadi resolusi 2 x 2 adalah sebagai berikut :



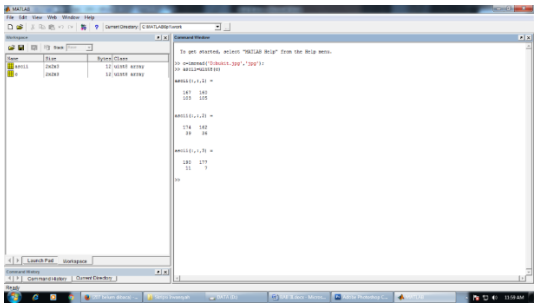
**Gambar 3.** Hasil Piksel 2x2

Dari citra di atas untuk menampilkan pixel pixel citra tersebut dengan menggunakan aplikasi matlab. Untuk menampilkan nilai matriks citra yang akan diolah dengan menggunakan bantuan aplikasi matlab dengan cara :

```
C= imread('D:bukit.jpg');
Ascii=uint8(c)
```

ISSN 2807-9507 (Media Online)
Vol 1, No 2, Desember 2021
Hal 67-74
https://djournals.com/jieee

Sehingga didapat nilai pixel citra di atas adalah sebagai berikut:



**Gambar 4.** Nilai Matriks Citra

2. Perintah untuk mengambil nilai warna RGB.

Ascii(…1) =R

| | |
|---|---|
| 167 | 160 |
| 103 | 105 |

Ascii (…2) = G

| | |
|---|---|
| 190 | 177 |
| 39 | 36 |

Ascii (…3) = B

| | |
|---|---|
| 181 | 162 |
| 11 | 7 |

3. Langkah selanjutnya ubah citra RGB ke *grayscale* ;

1. $f(1,1) = \frac{167+190+181}{3} = 179$
2. $f(1,2) = \frac{160+177+162}{3} = 166$
3. $f(2,1) = \frac{103+39+11}{3} = 51$
4. $f(2,2) = \frac{105+36+7}{3} = 49$

Maka nilai Ascii dari hasil konversi RGB ke G*rayscale* adalah:

| | |
|---|---|
| 179 | 166 |
| 51 | 49 |

**Gambar 5.** Hasil Konversi RGB Ke Grayscale

### 3.2 Penerapan Algoritma ElGamal dan Algoritma *Double Playfair Cipher*

Algoritma ElGamal merupakan salah satu penerapan algoritma asimetris, sehingga memiliki 2 buah kunci, yaitu kunci publik dan kunci privat.

1. Proses Pembangkitan Kunci
   Langkah-langkah dalam pembangkitan kunci.
   a. Pilih bilangan prima p besar sebagai basis grup perkalian (Z*p,x)
   b. Pilih α sebagai akar primitif pada grup
   c. Pilih d yang memenuhi $1 \leq d \leq p - 2$
2. Hitung berapa $\beta=\alpha^d \bmod p$
   Diperoleh kunci publik (p,α, β), kunci privat = d.
   a. Pilih bilangan prima p = 271

b. Pilih $\alpha$ =107
c. Pilih d = 96
d. $\beta = \alpha^d \bmod p$
   $=107^{96} \bmod 271$
   $= 39$

Hasil dari perhitungan diperoleh:
e. Kunci publik (p,$\alpha$, $\beta$) = (271, 107, 39)
f. Kunci privat (d)=(96)

3. Proses Enkripsi
   Langkah-langkah dalam mengenkripsi pesan:
   a. Terima kunci publik (p,$\alpha$, $\beta$) = (271, 107, 39).
   b. Plainteks m disusun menjadi blok-blok m1, m2, …, mp-1 sedemikian sehingga setiap blok merepresentasikan nilai di dalam rentang 0 sampai p – 1.
   c. Ubah nilai blok pesan ke dalam nilai ASCII. Ekspresikan pesan $P_1$ = C = 67 (ASCII) sebagai bilangan.
   d. Ambil sebuah bilangan asli r< p-1. Misal r = 50.
   e. Hitung $c_1 = \alpha^r \bmod p$.
      $= 107^{50} \bmod 271$
      $= 238$
      Hitung $c_2 = P_1 \times \beta^r \bmod p$
      $= 67 \times 39^{50} \bmod 271$
      $= 212$
      Maka dari perhitungan di atas, kita mendapatkan nilai $c_1$ dan $c_2$ sebagai cipherteks nya yaitu (238, 212). Proses diatas akan berulang untuk membaca semua blok pesan untuk menghasilkan cipherteks.
   f. Kirim $c_1$ = 238 dan $c_2$ = 212.

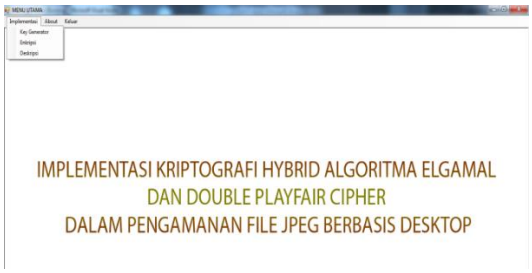
4. Proses Dekripsi
   Dalam mendeskripsi pesan digunakan perhitungan $P = c_2 \times (c_1^d)^{-1} \bmod p$. Perhitungan tersebut dapat disederhanakan dengan teorema Fermat:
   $P = c_2 \; x \; c_1^{p-1-d} \bmod p$
   Untuk memepermudah perhitungan pada tiap-tiap blok pesan, maka dapat dirumuskan dengan :
   $Z = c_1^{p-1-d} \bmod p$
   $P = c_2 \; x \; Z \bmod p$
   Langkah-langkah dalam mendekripsi pesan:
   a. Terima ($c_1$, $c_2$) dari sender = ( 238, 212)
   b. Hitung $Z = c_1^{p-1-d} \bmod p$
      $= 238^{271-1-96} \bmod 271$
      $= 238^{174} \bmod 271$
      $= 178$
      Hitung $P = c_2 \; x \; Z \bmod p$
      $= 212 \; x \; 178 \bmod 271$
      $= 67$
      Maka diperoleh P = 67, dalam karakter dalam ASCII adalah C, sesuai dengan plainteks yang dikirim sender.
   c. Kemudian menggabungkan blok m1, m2, menjadi plainteks yang utuh.

Kebutuhan sistem dalam mengimplementasikan program aplikasi yang telah dirancang diperlukan sebuah alat bantu berupa komputer, yang mana untuk mengoperasikan komputer memerlukan tiga buah komponen pendukung seperti hardware, software dan brainware.

### 3.3 Tampilan

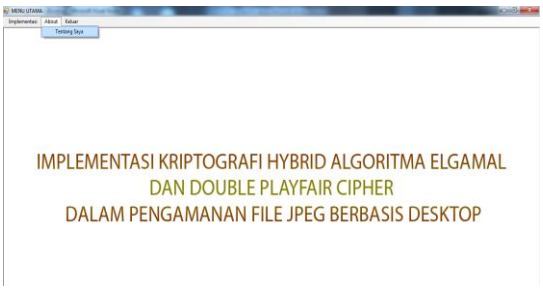
1. Menu Utama
   *Form* menu utama adalah antar muka (*interface*) yang digunakan sebagai *form* induk/*form* utama. *Form* utama ini akan selalu ditampilkan saat program dijalankan.

ISSN 2807-9507 (Media Online)
Vol 1, No 2, Desember 2021
Hal 67-74
https://djournals.com/jieee



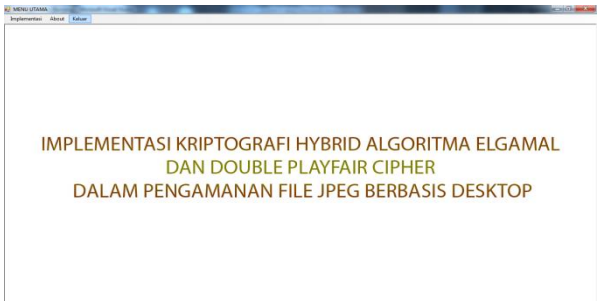

**Gambar 6.** Menu Utama

2. Tampilan Menu *About*
   Menu *about* terdiri dari satu submenu yaitu tentang saya yang berfungsi untuk menampilkan biodata tentang penulis. Tampilan submenu tentang saya dapat dilihat pada gambar sebagai berikut.



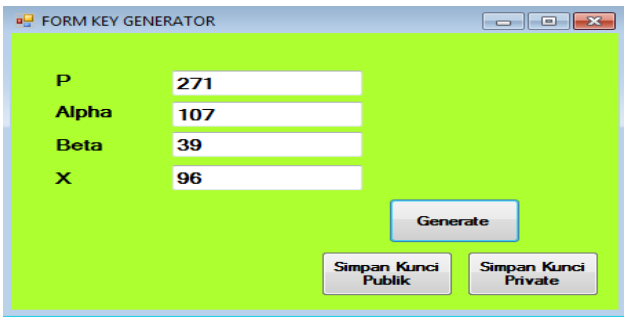

**Gambar 7.** Submenu Tentang Saya

3. Menu Keluar
   Menu keluar berfungsi untuk keluar dari program. Tampilan menu keluar dapat dilihat pada gambar sebagai berikut.




**Gambar 8.** Menu Keluar

4. *Form Key Generator*
   Tampilan *form key generator* digunakan untuk pembangkit kunci. *Form Key Generator* dapat dilihat pada gambar berikut ini.



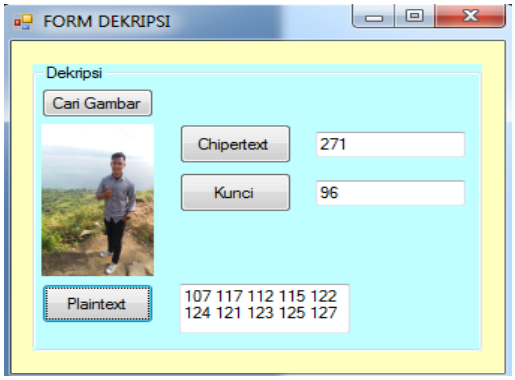

**Gambar 9.** *Form Key Generator*

ISSN 2807-9507 (Media Online)
Vol 1, No 2, Desember 2021
Hal 67-74
https://djournals.com/jieee

5. *Form* Enkripsi
   Tampilan *form* enkripsi dapat dilihat pada gambar sebagai berikut.


**Gambar 10.** *Form* Enkripsi

6. Form Dekripsi
   Tampilan *form* dekripsi dapat dilihat pada gambar sebagai berikut.




**Gambar 11.** *Form* Dekripsi

7 Form Tentang Saya
*Form* tentang saya digunakan untuk menampilkan biodata tentang penulis. Adapun tampilan *form* tentang saya dapat dilihat seperti pada gambar berikut ini.


**Gambar 12.** *Form* Tentang Saya

## 4. KESIMPULAN

Berdasarkan penelitian yang dilakukan maka di dapat sebuah kesimpulan bahwa dengan mengimplementasikan algoritma Elgamal dan algoritma *Double Playfair Cipher* diperoleh suatu aplikasi yang dapat mengamankan *file* citra. File citra diperkecil menjadi resolusi 2 x 2.

# REFERENCES

[1] Sadikin, Rifki, *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Yogyakarta : Andi, 2012

[2] Munir Rinaldi, Kriptografi, Bandung : Informatika, 2006

[3] A Widyartono, Algoritma Elgamal Untuk Enkripsi Data Menggunakan Gnupg. Jurnal Teknologi Dan Informatika (Teknomatika) 1(1): 29-35, 2011

[5] Ahmad Syawqi Lubis, *Analisis Perbandingan Metode Playfair Cipher Dan Elgamal Pada Kriptografi Citra*. Skripsi.Universitas Sumatera Utara, 2015

[6] Wiwin Agustini Lubis, *Penyandian Data Teks Dengan Algoritma Elgamal Dan Algoritma Kompresi Data Dengan Algoritma Elias Gamma Code*. Skripsi.Universitas Sumatera Utara, 2015

[7] Kromodimoeljo, Teori dan Aplikasi Kriptografi, Jakarta : SPK IT Consulting, 2009

[8] Munir Rinaldi, Pengolahan Citra digital dengan Pendekatan Algo, Bandung : Informatika, 2006

[9] M. Taufiq, Penerapan Algoritma Kriptografi Elgamal Untuk Pengaman File Citra, Jurnal EECCIS Vol. IV, No.1, Hal. 8-11, 2010

[10] Lubis, Ahmad Syawqi., Analisis Perbandingan Metode Playfair Cipher Dan Elgamal Pada Kriptografi Citra. Skripsi.Universitas Sumatera Utara, 2015

[11] Hendrayudi, Microsoft Visual Basic 2008, Bandung : Satu Nusa, 2011