Aplikasi Pengamanan File Gambar Menggunakan Algoritma Elgamal

Akim Manaor Hara Pardede[1*], Budi Serasi Ginting[2], Katen Lumbanbatu[3], Novriyenni[4], Yani Maulita[5], Achmad Fauzi[6] ,Nur Hidaya[7]

* Corresponding author : akimmhp@live.com
[1,2,3,4,5,6,7] Sekolah Tinggi Manajemen dan Informatika SMTIK Kaputama Binjai
Jl. Veteran No. 4A – 9A, Binjai, Sumatera Utara

Abstract--The growing use of information technology in helping human work in various types of activities involving computers as the media, then the issue of security and confidentiality is one very important aspect in the information system of a data, message, and information. Encryption is the best way to secure device and data information. In everyday codes are usually used to mean an encryption method or concealment of meaning. In cryptography, the elgamal algorithm can be used to encrypt and decrypt the image file. Elgamal algorithm can help maintain the security of image file so as to avoid the theft / damage to image file from irresponsible person.

Keywords-- Cryptography, Image Files, Elgamal Algorithm.

Abstrak-- Semakin berkembangnya pemanfaatan teknologi informasi dalam membantu pekerjaan manusia di berbagai jenis kegiatan yang melibatkan komputer sebagai medianya, maka masalah keamanan dan kerahasiaan merupakan salah satu aspek yang sangat penting dalam sistem informasi dari suatu data, pesan, dan informasi. Enkripsi adalah cara yang terbaik untuk mengamankan perangkat dan data informasi. Dalam sehari-hari kode biasanya digunakan untuk mengartikan suatu metode enkripsi atau penyembunyian suatu makna. Dalam ilmu kriptografi, algoritma elgamal dapat dimanfaatkan untuk melakukan enkripsi dan dekripsi pada file gambar. Algoritma Elgamal dapat membantu menjaga keamanan file gambar sehingga dapat terhindar dari pencurian/kerusakan pada file gambar dari orang yang tidak bertanggung jawab.

Kata Kunci-- Kriptografi, File Gambar, Algoritma Elgamal.

PENDAHULUAN

Dengan semakin berkembangnya pemanfaatan teknologi informasi dalam membantu pekerjaan manusia di berbagai jenis kegiatan yang melibatkan komputer sebagai medianya, maka masalah keamanan dan kerahasiaan merupakan salah satu aspek yang sangat penting dalam sistem informasi dari suatu data, pesan, dan informasi. Hingga zaman modern seperti ini, keamanan data semata-mata dianggap sebagai enkripsi, yaitu proses mengubah informasi yang tidak biasa dan tidak dapat dibaca menjadi suatu informasi yang jelas dan dapat dibaca. Enkripsi adalah cara yang terbaik untuk mengamankan perangkat dan data informasi. Dalam sehari-hari kode biasanya digunakan untuk mengartikan suatu metode enkripsi atau penyembunyian suatu makna.

Citra (*image*) atau gambar merupakan salah satu bentuk multimedia yang penting. Citra yang disimpan atau yang akan ditransmisikan dalam bentuk *plainimage* / gambar yang akan dienkripsi rentan dalam bentuk penyadapan dan pencurian. Algoritma Elgamal termasuk dalam kriptografi modern yang menggunakan *plaintext*, *ciphertext* dan kunci untuk melakukan proses enkripsi dan

dekripsi dalam pengamanan data. 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.

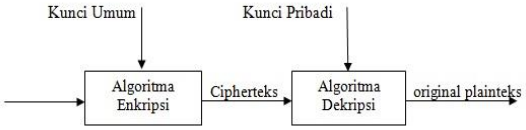
Tujuan penyusunan penelitian ini adalah sebagai berikut : Untuk membantu menjaga keamanan *file* gambar dengan menggunakan algoritma Elgamal agar terhindar dari pencurian/kerusakan pada *file* gambar dari orang yang tidak bertanggung jawab.

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga.

Menurut Sentot Kromodimoeljo (2009, h.5) Kriptografi adalah ilmu yang mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekrip untuk mendapatkan kembali data asli. Walaupun awalnya kriptografi digunakan untuk merahasiakan naskah berupa teks, kini kriptografi digunakan untuk data apa saja yang berbentuk digital. [1]

Menurut (Dony Aryius. 2008), Kriptografi berasal dari bahasa Yunani yaitu *cryptos* yang berarti rahasia dan *graphein* artinya tulisan. Jadi kriptografi berarti tulisan rahasia. Secara istilah kriptografi didefenisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang mempunyai arti atau nilai, dengan cara menyamarkannya (mengacak) menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu menurut *Bruce Scheiner*, kriptografi adalah ilmu pengetahuan dan seni menjaga pesan-pesan agar tetap aman. Sedangkan menurut *Menezer*, kriptografi adalah ilmu yang mempelajari teknik-teknik matematik yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi. Pesan atau informasi dapat dikategorikan kedalam dua jenis, yaitu pesan yang dapat dibaca dengan mudah (*plaintext*) dan pesan yang tidak mudah dibaca (*ciphertext*). [2]

Kunci Umum Kunci Pribadi



Gambar 1. *Konsep Dasar dari Enkripsi dan Dekripsi*

Pada konsep dasar enkripsi dan dekripsi pada gambar II.2 dimana setiap pelaku sistem informasi akan memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi, dimana kunci publik di distribusikan kepada umum, sedangkan kunci pribadi disimpan untuk diri sendiri. artinya bila plainteks ingin mengirimkan pesan kepada cipherteks, plainteks dapat menyandikan pesannya dengan menggunakan kunci publik cipherteks, dan bila cipherteks ingin membaca surat tersebut, ia perlu mendeskripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut.

Dari penelitian Jurnal KAPUTAMA, Vol.8 No.1, Juli 2014 yang berkaitan dengan penerapan enkripsi yang diteliti oleh ***Akim Manaor Hara Pardede dan Yani Maulita*** dengan judul ***Perancangan Perangkat Lunak Enkripsi Dan Deskripsi File Dengan Metode Transposisi Kolom*** dengan kesimpulan dari penelitian ini adalah Perancangan perangkat lunak enkripsi kata sandi dengan metode Transposisi Kolom yang dirancang memiliki kelemahan yaitu pada penentuan kata sandi. Walaupun kata sandi yang di inputkan user berbeda dengan kata sandi utama, namun posisi kolom kata kuncinya sesuai, maka pesan enkripsi tetap dapat di lakukan dengan hasil yang sama (Pardede & Maulita, 2014). [3]

Suatu sistem yang mampu melindungi data dan merahasiakannya dengan menggunakan berbagai algoritma, salah satunya adalah algoritma Vigenere Cipher dan Hill Cipher, atau Elgamal, setiap aplikasi yang dibangun selain dapat digunakan sebagai alat pengaman data dokumen dapat juga digunakan sebagai aplikasi pembelajaran algoritma(Pardede, 2017). [4]

Algoritma Elgamal

Algoritma elgamal ditemukan pada tahun 1985 oleh ilmuwan Mesir yaitu *Taher Elagamal*. Algoritma elgamal merupakan algoritma

berdasarkan konsep kunci publik. Algoritma ini pada umumnya digunakan untuk *digital signature*, namun kemudian dimodifikasi sehingga bisa digunakan untuk enkripsi dan dekripsi.

Menurut (Sentot Kromodimoeljo, 2010) keamanan algoritma elgamal terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sulit untuk dipecahkan. Algoritma ini memiliki kelebihan yaitu pembangkitan kunci yang menggunakan logaritma diskrit dan metode enkripsi dan dekripsi yang menggunakan proses komputasi yang besar sehingga hasil enkripsi nya berukuran dua kali dari ukuran semula. Kekurangan algoritma ini adalah membutuhkan *resource* yang besar sehingga hasil enkripsi nya berukuran dua kali dari ukuran semula. Kekurangan algoritma ini adalah membutuhkan resource yang besar karena cipherteks yang dihasilkan dua kali panjang plainteks serta membutuhkan procesor yang mampu untuk melakukan komputasi yang besar untuk perhitungan logaritma perpangkatan besar. [5]

Secara garis besar algoritma elgamal mempunyai langkah-langkah pembentukan kunci sebagai berikut :

Bilangan prima, p (bersifat *public* atau tidak rahasia).

Bilangan acak, g (dimana x < p dan bersifat *private* atau rahasia).

Bilangan acak, x (dimana x < p dan bersifat *private* atau rahasia).

Bilangan acak, k (dimana k < p dan bersifat *private* atau rahasia).

m merupakan plainteks dan bersifat *private* / rahasia. a dan b merupakan pasangan cipherteks hasil enkripsi bersifat *private* atau tidak rahasia.

Proses pembentukan kunci algoritma elgamal, proses pembentukan kunci merupakan proses penentuan suatu bilangan yang kemudian akan digunakan sebagai kunci pada proses enkripsi dan dekripsi pesan. Kunci untuk enkripsi dibangkitkan dari nilai p, g, y sedangkan kunci untuk dekripsi terdiri dari nilai x, p. Masing – masing nilai mempunyai persyaratan yang harus dipenuhi.

Langkah –langkah dalam pembuatan kunci adalah sebagai berikut :

1. Pilih sembarang bilangan prima p, dengan syarat p > 211.
2. Pilih bilangan acak g dengan syarat g < p.
3. Pilih bilangan acak x dengan syarat $1 \leq x \leq p-2$.
4. Hitung $y = g^{\wedge x}$ *mod* p.

ANALISA PERHITUNGAN ALGORITMA ELGAMAL

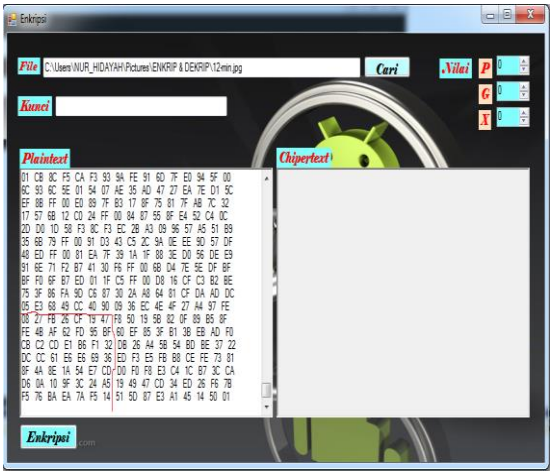
Proses file gambar matriks 7x7 tersebut adalah :

Adapun gambar yang dipilih untuk mengambil nilai acsii hexadesimal sebagai berikut :

Gambar 2. *File Gambar Format jpg*

Gambar 2 merupakan gambar yang akan dilakukan enkripsi, langkah awal penulis mengambil nilai ascii hexadesimal dari file gambar yang akan di enkripsi, karena nilai yang dihasilkan sangat banyak. Maka sampel yang diambil hanya matriks 7x7 berikut adalah hasil nilai acsii hexadesimal yang didapat.

Berikut adalah hasil dari nilai ascii hexadesimal pada file gambar yang telah dikonvert :



Gambar 3. *Hasil Pengambilan Nilai Ascii Hexadesimal*

Tabel dibawah adalah hasil nilai asciii hexadesimal yang di peroleh, matriks 10x10 yang akan dienkripsi *(Plaintext)* :

Tabel 1. *Tabel Hasil Convert File Gambar ke Hexadesimal Matriks 7x7*

o							
	8	7	B	6	F	9	7
	E	B	F	2	D	5	F
	B	2	D	1	6	1	2
	C	C	1	6	6	9	6
	F	A	E	A	4	7	D
	6	A	0	F	C	4	5
	5	6	A	A	A	5	4

Setelah mendapatkan nilai ascii hexadesimal, berikutnya melakukan enkripsi dan dekripsi dengan algoritma elgamal.

A. Tahap Enkripsi

File gambar akan di potong menjadi blok – blok bilangan hexadesimal dan di konversikan ke dalam bilangan ASCII.

Tabel 2. *Konversi hexadesimal File Gambar ke Dalam Kode ASCII Desimal*

o	**Bilangan Hexadesimal**	**Plainteks Mi**	**Plainteks mi (ASCII Desimal)**
	08	M_1	8
	27	M_2	39
	FB	M_3	251
	26	M_4	38
	CF	M_5	207
	19	M_6	25
	47	M_7	71
	FE	M_8	254
	4B	M_9	75
0	AF	M_{10}	175
1	62	M_{11}	98
2	FD	M_{12}	253
3	95	M_{13}	149
4	BF	M_{14}	191
5	CB	M_{15}	203
6	C2	M_{16}	194
7	CD	M_{17}	205
8	E1	M_{18}	225
9	B6	M_{19}	182
0	F1	M_{20}	241
1	32	M_{21}	50
2	DC	M_{22}	220
3	CC	M_{23}	204
4	61	M_{24}	97
5	E6	M_{25}	230
6	E6	M_{26}	230
7	69	M_{27}	105
8	36	M_{28}	54
9	8F	M_{29}	143
0	4A	M_{30}	74
1	8E	M_{31}	142
2	1A	M_{32}	26
3	54	M_{33}	84
4	E7	M_{34}	231
5	CD	M_{35}	205
6	D6	M_{36}	214
7	0A	M_{37}	10
8	10	M_{38}	16
9	9F	M_{39}	159
0	3C	M_{40}	60
1	24	M_{41}	36
2	A5	M_{42}	165

3	F5	M_{43}	245
4	76	M_{44}	118
5	BA	M_{45}	186
6	EA	M_{46}	234
7	7A	M_{47}	122
8	F5	M_{48}	245
9	14	M_{49}	20

Proses menentukan bilangan acak $P \in \{0,1, \ldots \ldots \ldots .233\}$

Tabel 3. *Menentukan Bilangan Acak Kunci*

No	Mn	Nilai	Kunci
1	M_1	8	19
2	M_2	39	35
3	M_3	251	15
4	M_4	38	13
5	M_5	207	21
6	M_6	25	33
7	M_7	71	17
8	M_8	254	53
9	M_9	75	67
10	M_{10}	175	71
11	M_{11}	98	73
12	M_{12}	253	89
13	M_{13}	149	79
14	M_{14}	191	63
15	M_{15}	203	67
16	M_{16}	194	41
17	M_{17}	205	53
18	M_{18}	225	27
19	M_{19}	182	77
20	M_{20}	241	43
21	M_{21}	50	21
22	M_{22}	220	59
23	M_{23}	204	29
24	M_{24}	97	35
25	M_{25}	230	81
26	M_{26}	230	89
27	M_{27}	105	75
28	M_{28}	54	85
29	M_{29}	143	73
30	M_{30}	74	55
31	M_{31}	142	69
32	M_{32}	26	91
33	M_{33}	84	31
34	M_{34}	231	43
35	M_{35}	205	53
36	M_{36}	214	97
37	M_{37}	10	93
38	M_{38}	16	71
39	M_{39}	159	59
40	M_{40}	60	63
41	M_{41}	36	65
42	M_{42}	165	69
43	M_{43}	245	79
44	M_{44}	118	81
45	M_{45}	186	23
46	M_{46}	234	51
47	M_{47}	122	25
48	M_{48}	245	61
49	M_{49}	20	91

kemudian mencari nilai $\boldsymbol{y}$ dan nilai $\boldsymbol{mi}$
Dengan rumus :

$$\boldsymbol{y \equiv g^x \bmod p} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

$$\boldsymbol{mi \equiv b1.a1^{p-1-x} \bmod p} \ldots\ldots\ldots\ldots\ldots \quad (2)$$

Sebelum mencari nilai y dan nilai m_i , misalkan acak membangkitkan pasangan kunci dengan memilih bilangan:
Dimana P = Prima
g = bilangan acak (tidak rahasia)
x = bilangan acak (rahasia/ private)
p=23
g=13
x = 11

Kemudian p, g, x digunakan untuk menghitung nilai y :
Dengan Rumus :

$$\boldsymbol{y \equiv g^x \bmod p} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

$$y \equiv 13^{11} \bmod 233$$
$$\boldsymbol{y \equiv 207}$$

Hasil algoritma nya adalah :
kunci publik adalah triple (207, 13, 233)
kunci private adalah pasangan (11, 233)
dimana mencari Enkripsi a adalah :
Dengan rumus :

$$\boldsymbol{a \equiv g^{ki} \bmod p} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

$\boldsymbol{a \equiv g^{ki} \bmod p}$

$a1 \equiv 13^{19} \bmod 233$

$\boldsymbol{a1 \equiv 72}$

$a2 \equiv 13^{35} \bmod 233$

$\boldsymbol{a2 \equiv 173}$

$a3 \equiv 13^{15} \bmod 233$

$\boldsymbol{a3 \equiv 218}$

$a4 \equiv 13^{13} \bmod 233$

$\boldsymbol{a4 \equiv 33}$

$a5 \equiv 13^{21} \bmod 233$

$\boldsymbol{a5 \equiv 52}$

$a6 \equiv 13^{33} \bmod 233$

$\boldsymbol{a6 \equiv 132}$

$a7 \equiv 13^{17} \bmod 233$

$\boldsymbol{a7 \equiv 28}$

$a8 \equiv 13^{53} \bmod 233$

$\boldsymbol{a8 \equiv 62}$

$a9 \equiv 13^{67} \bmod 233$

$\boldsymbol{a9 \equiv 36}$

$a10 \equiv 13^{71} \bmod 233$

$\boldsymbol{a10 \equiv 200}$

$a11 \equiv 13^{73} \bmod 233$

$\boldsymbol{a11 \equiv 15}$

$a12 \equiv 13^{89} \bmod 233$

$\boldsymbol{a12 \equiv 104}$

$a13 \equiv 13^{79} \bmod 233$

$\boldsymbol{a13 \equiv 181}$

$a14 \equiv 13^{63} \bmod 233$

$\boldsymbol{a14 \equiv 109}$

$a15 \equiv 13^{67} \bmod 233$

$\boldsymbol{a15 \equiv 36}$

$a16 \equiv 13^{41} \bmod 233$

$\boldsymbol{a16 \equiv 208}$

$a17 \equiv 13^{53} \bmod 233$

$\boldsymbol{a17 \equiv 62}$

$a18 \equiv 13^{27} \bmod 233$

$\boldsymbol{a18 \equiv 177}$

$a19 \equiv 13^{77} \bmod 233$

$\boldsymbol{a19 \equiv 161}$

$a20 \equiv 13^{43} \bmod 233$

$\boldsymbol{a20 \equiv 202}$

$a21 \equiv 13^{21} \bmod 233$

$\boldsymbol{a21 \equiv 52}$

$a22 \equiv 13^{59} \bmod 233$

$\boldsymbol{a22 \equiv 220}$

$a23 \equiv 13^{29} \bmod 233$

$\boldsymbol{a23 \equiv 89}$

$a24 \equiv 13^{35} \bmod 233$

$\boldsymbol{a24 \equiv 173}$

$a25 \equiv 13^{81} \bmod 233$

$\boldsymbol{a25 \equiv 66}$

$a26 \equiv 13^{89} \bmod 233$

$\boldsymbol{a26 \equiv 104}$

$a27 \equiv 13^{75} \bmod 233$

$\boldsymbol{a27 \equiv 205}$

$a28 \equiv 13^{85} \bmod 233$

$\boldsymbol{a28 \equiv 56}$

$a29 \equiv 13^{73} \bmod 233$

$\boldsymbol{a29 \equiv 15}$

$a30 \equiv 13^{55} \bmod 233$

$\boldsymbol{a30 \equiv 226}$

$a31 \equiv 13^{69} \bmod 233$

$\boldsymbol{a31 \equiv 26}$

$a32 \equiv 13^{91} \bmod 233$

$\boldsymbol{a32 \equiv 109}$

$a33 \equiv 13^{31} \bmod 233$

$\boldsymbol{a33 \equiv 129}$

$a34 \equiv 13^{43} \bmod 233$

$\boldsymbol{a34 \equiv 202}$

$a35 \equiv 13^{53} \bmod 233$

$\boldsymbol{a35 \equiv 62}$

$a36 \equiv 13^{97} \bmod 233$

$\boldsymbol{a36 \equiv 178}$

$a37 \equiv 13^{93} \bmod 233$

$\boldsymbol{a37 \equiv 60}$

$a38 \equiv 13^{71} \bmod 233$

$\boldsymbol{a38 \equiv 200}$

$a39 \equiv 13^{59} \bmod 233$

$\boldsymbol{a39 \equiv 220}$

$a40 \equiv 13^{63} \bmod 233$

$\boldsymbol{a40 \equiv 109}$

$a41 \equiv 13^{65} \bmod 233$

$\boldsymbol{a41 \equiv 14}$

$a42 \equiv 13^{69} \bmod 233$

$\boldsymbol{a42 \equiv 26}$

$a43 \equiv 13^{79} \bmod 233$

$\boldsymbol{a43 \equiv 181}$

$a44 \equiv 13^{81} \bmod 233$

$\boldsymbol{a44 \equiv 66}$

$a45 \equiv 13^{23} \bmod 233$

$\boldsymbol{a45 \equiv 167}$

$a46 \equiv 13^{51} \bmod 233$

$\boldsymbol{a46 \equiv 50}$

$a47 \equiv 13^{25} \bmod 233$

$\boldsymbol{a47 \equiv 30}$

$a48 \equiv 13^{61} \bmod 233$

$\boldsymbol{a48 \equiv 133}$

$a49 \equiv 13^{91} \bmod 233$

$\boldsymbol{a49 \equiv 101}$

dimana Enkripsi b adalah :

$\boldsymbol{b \equiv y^{ki} m . \bmod p}$

$b1 \equiv 207^{19}\, 8 \bmod 233$

$\boldsymbol{b1} \equiv \mathbf{14}$
$b2 \equiv 207^{35}\ 39\ mod\ 233$
$\boldsymbol{b2} \equiv \mathbf{174}$
$b3 \equiv 207^{15}\ 251\ mod\ 233$
$\boldsymbol{b3} \equiv \mathbf{117}$
$b4 \equiv 207^{13}\ 38\ mod\ 233$
$\boldsymbol{b4} \equiv \mathbf{202}$
$b5 \equiv 207^{21}\ 207\ mod\ 233$
$\boldsymbol{b5} \equiv \mathbf{231}$
$b6 \equiv 207^{33}\ 25\ mod\ 233$
$\boldsymbol{b6} \equiv \mathbf{91}$
$b7 \equiv 207^{17}\ 71\ mod\ 233$
$\boldsymbol{b7} \equiv \mathbf{220}$
$b8 \equiv 207^{53}\ 254\ mod\ 233$
$\boldsymbol{b8} \equiv \mathbf{3}$
$b9 \equiv 207^{67}\ 75\ mod\ 233$
$\boldsymbol{b9} \equiv \mathbf{222}$
$b10 \equiv 207^{71}\ 175\ mod\ 233$
$\boldsymbol{b10} \equiv \mathbf{14}$
$b11 \equiv 207^{73}\ 98\ mod\ 233$
$\boldsymbol{b11} \equiv \mathbf{62}$
$b12 \equiv 207^{89}\ 253\ mod\ 233$
$\boldsymbol{b12} \equiv \mathbf{68}$
$b13 \equiv 207^{79}\ 149\ mod\ 233$
$\boldsymbol{b13} \equiv \mathbf{114}$
$b14 \equiv 207^{63}\ 191\ mod\ 233$
$\boldsymbol{b14} \equiv \mathbf{172}$
$b15 \equiv 207^{67}\ 203\ mod\ 233$
$\boldsymbol{b15} \equiv \mathbf{51}$
$b16 \equiv 207^{41}\ 194\ mod\ 233$
$\boldsymbol{b16} \equiv \mathbf{20}$
$b17 \equiv 207^{53}\ 205\ mod\ 233$
$\boldsymbol{b17} \equiv \mathbf{229}$
$b18 \equiv 207^{27}\ 225\ mod\ 233$
$\boldsymbol{b18} \equiv \mathbf{121}$
$b19 \equiv 207^{77}\ 182\ mod\ 233$
$\boldsymbol{b19} \equiv \mathbf{31}$
$b20 \equiv 207^{43}\ 241\ mod\ 233$
$\boldsymbol{b20} \equiv \mathbf{178}$
$b21 \equiv 207^{21}\ 50\ mod\ 233$
$\boldsymbol{b21} \equiv \mathbf{201}$
$b22 \equiv 207^{59}\ 220\ mod\ 233$
$\boldsymbol{b22} \equiv \mathbf{128}$
$b23 \equiv 207^{29}\ 204\ mod\ 233$
$\boldsymbol{b23} \equiv \mathbf{18}$
$b24 \equiv 207^{35}\ 97\ mod\ 233$
$\boldsymbol{b24} \equiv \mathbf{146}$
$b25 \equiv 207^{81}\ 230\ mod\ 233$
$\boldsymbol{b25} \equiv \mathbf{156}$
$b26 \equiv 207^{89}\ 230\ mod\ 233$
$\boldsymbol{b26} \equiv \mathbf{156}$
$b27 \equiv 207^{75}\ 105\ mod\ 233$
$\boldsymbol{b27} \equiv \mathbf{203}$
$b28 \equiv 207^{85}\ 54\ mod\ 233$
$\boldsymbol{b28} \equiv \mathbf{176}$
$b29 \equiv 207^{73}\ 143\ mod\ 233$
$\boldsymbol{b29} \equiv \mathbf{119}$
$b30 \equiv 207^{55}\ 74\ mod\ 233$
$\boldsymbol{b30} \equiv \mathbf{123}$
$b31 \equiv 207^{69}\ 142\ mod\ 233$
$\boldsymbol{b31} \equiv \mathbf{100}$
$b32 \equiv 207^{91}\ 26\ mod\ 233$
$\boldsymbol{b32} \equiv \mathbf{157}$
$b33 \equiv 207^{31}\ 84\ mod\ 233$
$\boldsymbol{b33} \equiv \mathbf{227}$
$b34 \equiv 207^{43}\ 231\ mod\ 233$
$\boldsymbol{b34} \equiv \mathbf{72}$
$b35 \equiv 207^{53}\ 205\ mod\ 233$
$\boldsymbol{b35} \equiv \mathbf{229}$
$b36 \equiv 207^{97}\ 214\ mod\ 233$
$\boldsymbol{b36} \equiv \mathbf{89}$
$b37 \equiv 207^{93}\ 10\ mod\ 233$
$\boldsymbol{b37} \equiv \mathbf{45}$
$b38 \equiv 207^{71}\ 16\ mod\ 233$
$\boldsymbol{b38} \equiv \mathbf{197}$
$b39 \equiv 207^{59}\ 159\ mod\ 233$
$\boldsymbol{b39} \equiv \mathbf{173}$
$b40 \equiv 207^{63}\ 60\ mod\ 233$
$\boldsymbol{b40} \equiv \mathbf{187}$
$b41 \equiv 207^{65}\ 36\ mod\ 233$
$\boldsymbol{b41} \equiv \mathbf{29}$
$b42 \equiv 207^{69}\ 165\ mod\ 233$
$\boldsymbol{b42} \equiv \mathbf{44}$
$b43 \equiv 207^{79}\ 245\ mod\ 233$
$\boldsymbol{b43} \equiv \mathbf{97}$
$b44 \equiv 207^{81}\ 118\ mod\ 233$
$\boldsymbol{b44} \equiv \mathbf{155}$
$b45 \equiv 207^{23}\ 186\ mod\ 233$
$\boldsymbol{b45} \equiv \mathbf{119}$
$b46 \equiv 207^{51}\ 234\ mod\ 233$
$\boldsymbol{b46} \equiv \mathbf{178}$
$b47 \equiv 207^{25}\ 122\ mod\ 233$
$\boldsymbol{b47} \equiv \mathbf{179}$
$b48 \equiv 207^{61}\ 98\ mod\ 233$
$\boldsymbol{b48} \equiv \mathbf{112}$
$b49 \equiv 207^{91}\ 20\ mod\ 233$
$\boldsymbol{b49} \equiv \mathbf{67}$

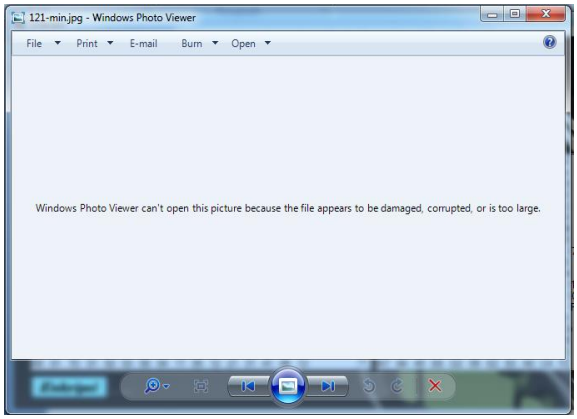
Setelah mendapatkan nilai enkripsi a dan b, hasil perhitungan tersebut disusun dengan pola selang seling:

a1, b1, a2, b2, a3, b3, a4, b4, a5, b5, a6, b6, a7, b7, a8, b8, a9, b9, a10, b10, a11, b11, a12, b12,

a13, b13, a14, b14, a15, b15, a16, b16, a17, b17, a18, b18, a19, b19, a20, b20, a21, b21, a22, b22, a23, b23, a24, b24, a25, b25, a26, b26, a27, b27, a28, b28, a29, b29, a30, b30, a31, b31, a32, b32, a33, b33, a34, b34, a35, b35, a36, b36, a37, b37, a38, b38, a39, b39, a40, b40, a41, b41, a42, b42, a43, b43, a44, b44, a45, b45, a46, b46, a47, b47, a48, b48, a49, b49.

Sehingga membentuk cipherteks :
72, 14, 173, 174, 218, 117, 33, 202, 52, 231, 132, 91, 28, 220, 62, 3, 36, 222, 200, 14, 15, 62, 104, 68, 181, 114, 109, 172, 36, 51, 208, 20, 62, 229, 177, 121, 161, 31, 202, 178, 52, 201, 220, 128, 89, 18, 173, 146, 66, 156, 104, 156, 205, 203, 56, 176, 15, 119, 226, 123, 26, 100, 109, 157, 129, 227, 202, 72, 62, 229, 178, 89, 60, 45, 200, 197, 220, 173, 109, 187, 14, 29, 26, 44, 181, 97, 66, 155, 167, 119, 50, 178, 30, 179, 133, 112, 101, 67.

Di dalam bentuk karakter menjadi :
H, <, -, ®, Ú, u, !, Ê, 4, ç, „, [, FS, Ü, >, ETX, $, Þ, È, SO, SI, >, h, D, µ, r, m, ¬, $, 3, Ð, DC4, >, å, ±, y, ¡, US, Ê, ², 4, É, Ü, €, Y, DC2, -, ', B, œ, h, œ, Í, Ë, 8, °, SI,w, â, {, SUB, d, m, OSC, ã, Ê, H, >, å, ², Y, <, -, È, Å, Ü, -, m, », , SO, GS, SUB, ,µ, a, B, ›, §, w, 2, ², RS, ³, NEL, p, e, C (Dalam Bilangan Ascii)
Hasil ciphertext tidak akan dapat dikenali, seperti sampel gambar berikut ini:



Gambar 4. *Hasil ciphertext gambar setelah dienkripsi*

B. Tahap Dekripsi
Cipherteks akan di potong menjadi blok – blok karakter dan di konversikan ke dalam bilangan ASCII.

Tabel 4. *Konversi Blok Cipherteks ke dalam kode* **ASCII**

No	Karakter	Plainteks Mi	Plainteks mi (ASCII)
1	H	M_1	72
2	<	M_2	14
3	-	M_3	173
4	®	M_4	174
5	Ú	M_5	218
6	u	M_6	117
7	!	M_7	33
8	Ê	M_8	202
9	4	M_9	52
10	ç	M_{10}	231
11	„	M_{11}	132
12	[	M_{12}	91
13	FS	M_{13}	28
14	Ü	M_{14}	220
15	>	M_{15}	62
16	ETX	M_{16}	3
17	$	M_{17}	36
18	Þ	M_{18}	222
19	È	M_{19}	200
20	SO	M_{20}	14
21	SI	M_{21}	15
22	>	M_{22}	62
23	h	M_{23}	104
24	D	M_{24}	68
25	µ	M_{25}	181
26	r	M_{26}	114
27	M	M_{27}	109
28	¬	M_{28}	172
29	$	M_{29}	36
30	3	M_{30}	51
31	Ð	M_{31}	208
32	DC4	M_{32}	20
33	>	M_{33}	62
34	å	M_{34}	229
35	±	M_{35}	177
36	y	M_{36}	121
37	¡	M_{37}	161
38	US	M_{38}	31
39	Ê	M_{39}	202
40	²	M_{40}	178
41	4	M_{41}	52
42	É	M_{42}	201
43	Ü	M_{43}	220
44	€	M_{44}	128

45	Y	M_{45}	89
46	DC2	M_{46}	18
47	-	M_{47}	173
48	’	M_{48}	146
49	B	M_{49}	66
50	œ	M_{50}	156
51	h	M_{51}	104
52	œ	M_{52}	156
53	Í	M_{53}	205
54	Ë	M_{54}	203
55	8	M_{55}	56
56	°	M_{56}	176
57	SI	M_{57}	15
58	w	M_{58}	119
59	â	$M59$	226
60	{	M_{60}	123
61	SUB	M_{61}	26
62	d	M_{62}	100
63	m	M_{63}	109
64	OSC	M_{64}	157
65		M_{65}	129
66	ã	M_{66}	227
67	Ê	M_{67}	202
68	H	M_{68}	72
69	>	M_{69}	62
70	å	M_{70}	229
71	²	M_{71}	178
72	Y	M_{72}	89
73	<	M_{73}	60
74	-	M_{74}	45
75	È	M_{75}	200
76	Å	M_{76}	197
77	Ü	M_{77}	220
78	-	M_{78}	173
79	m	M_{79}	109
80	»	M_{80}	187
81	SO	M_{81}	14
82	GS	M_{82}	29
83	SUB	M_{83}	26
84	,	M_{84}	44
85	µ	M_{85}	181
86	a	M_{86}	97
87	B	M_{87}	66
88	CSI	M_{88}	155
89	§	M_{89}	167
90	w	M_{90}	119
91	2	M_{91}	50
92	²	M_{92}	178
93	RS	M_{93}	30
94	³	M_{94}	179
95	NEL	M_{95}	133
96	p	M_{96}	112
97	e	M_{97}	101
98	C	M_{98}	67

Selanjutnya mendekripsikan chiperteks dari B dengan melakukan perhitungan dengan rumus sebagai berikut :

$$\boldsymbol{cn \equiv bi.ai^{p-1-x}\ mod\ p} \quad \text{.....(5)}$$

$c1 \equiv 14.72^{233-1-11}\ mod\ 233$

$c1 \equiv 14.72^{221}\ mod\ 233$

$\boldsymbol{c1 \equiv 8}$

$c2 \equiv 174.173^{233-1-11}\ mod\ 233$

$c2 \equiv 174.173^{221}\ mod\ 233$

$\boldsymbol{c2 \equiv 39}$

$c3 \equiv 117.218^{233-1-11}\ mod\ 233$

$c3 \equiv 117.218^{221}\ mod\ 233$

$\boldsymbol{c3 \equiv 251}$

$c4 \equiv 202.33^{233-1-11}\ mod\ 233$

$c4 \equiv 202.33^{221}\ mod\ 233$

$\boldsymbol{c4 \equiv 38}$

$c5 \equiv 231.52^{233-1-11}\ mod\ 233$

$c5 \equiv 231.52^{221}\ mod\ 233$

$\boldsymbol{c5 \equiv 207}$

$c6 \equiv 91.132^{233-1-11}\ mod\ 233$

$c6 \equiv 91.132^{221}\ mod\ 233$

$\boldsymbol{c6 \equiv 25}$

$c7 \equiv 220.28^{233-1-11}\ mod\ 233$

$c7 \equiv 220.28^{221}\ mod\ 233$

$\boldsymbol{c7 \equiv 71}$

$c8 \equiv 3.62^{233-1-11}\ mod\ 233$

$c8 \equiv 3.62^{221}\ mod\ 233$

$\boldsymbol{c8 \equiv 254}$

$c9 \equiv 222.36^{233-1-11}\ mod\ 233$

$c9 \equiv 222.36^{221}\ mod\ 233$

$\boldsymbol{c9 \equiv 75}$

$c10 \equiv 14.200^{233-1-11}\ mod\ 233$

$c10 \equiv 14.200^{221}\ mod\ 233$

$\boldsymbol{c10 \equiv 175}$

$c11 \equiv 62.15^{233-1-11}\ mod\ 233$

$c11 \equiv 62.15^{221}\ mod\ 233$

$\boldsymbol{c11 \equiv 98}$

$c12 \equiv 68.104^{233-1-11}\ mod\ 233$

$c12 \equiv 68.104^{221}\ mod\ 233$

$\boldsymbol{c12 \equiv 253}$

$c13 \equiv 114.181^{233-1-11}\ mod\ 233$

$c13 \equiv 114.181^{221}\ mod\ 233$

$\boldsymbol{c13 \equiv 149}$

$c14 \equiv 172.109^{233-1-11}\ mod\ 233$

$c14 \equiv 172.109^{221} \ mod\ 233$

$\boldsymbol{c14 \equiv 191}$

$c15 \equiv 51.36^{233-1-11} \ mod\ 233$

$c15 \equiv 51.36^{221} \ mod\ 233$

$\boldsymbol{c15 \equiv 203}$

$c16 \equiv 20.208^{233-1-11} \ mod\ 233$

$c16 \equiv 20.208^{221} \ mod\ 233$

$\boldsymbol{c16 \equiv 194}$

$c17 \equiv 229.62^{233-1-11} \ mod\ 233$

$c17 \equiv 229.62^{221} \ mod\ 233$

$\boldsymbol{c17 \equiv 205}$

$c18 \equiv 14.177^{233-1-11} \ mod\ 233$

$c18 \equiv 14.177^{221} \ mod\ 233$

$\boldsymbol{c18 \equiv 225}$

$c19 \equiv 31.161^{233-1-11} \ mod\ 233$

$c19 \equiv 31.161^{221} \ mod\ 233$

$\boldsymbol{c19 \equiv 182}$

$c20 \equiv 178.202^{233-1-11} \ mod\ 233$

$c20 \equiv 178.202^{221} \ mod\ 233$

$\boldsymbol{c20 \equiv 241}$

$c21 \equiv 201.52^{233-1-11} \ mod\ 233$

$c21 \equiv 201.52^{221} \ mod\ 233$

$\boldsymbol{c21 \equiv 50}$

$c22 \equiv 128.220^{233-1-11} \ mod\ 233$

$c22 \equiv 128.220^{221} \ mod\ 233$

$\boldsymbol{c22 \equiv 220}$

$c23 \equiv 18.89^{233-1-11} \ mod\ 233$

$c23 \equiv 18.89^{221} \ mod\ 233$

$\boldsymbol{c23 \equiv 204}$

$c24 \equiv 146.173^{233-1-11} \ mod\ 233$

$c24 \equiv 146.173^{221} \ mod\ 233$

$\boldsymbol{c24 \equiv 97}$

$c25 \equiv 156.66^{233-1-11} \ mod\ 233$

$c25 \equiv 156.66^{221} \ mod\ 233$

$\boldsymbol{c25 \equiv 230}$

$c26 \equiv 156.104^{233-1-11} \ mod\ 233$

$c26 \equiv 156.104^{221} \ mod\ 233$

$\boldsymbol{c26 \equiv 230}$

$c27 \equiv 203.205^{233-1-11} \ mod\ 233$

$c27 \equiv 203.205^{221} \ mod\ 233$

$\boldsymbol{c27 \equiv 105}$

$c28 \equiv 176.56^{233-1-11} \ mod\ 233$

$c28 \equiv 176.56^{221} \ mod\ 233$

$\boldsymbol{c28 \equiv 54}$

$c29 \equiv 119.15^{233-1-11} \ mod\ 233$

$c29 \equiv 119.15^{221} \ mod\ 233$

$\boldsymbol{c29 \equiv 143}$

$c30 \equiv 123.226^{233-1-11} \ mod\ 233$

$c30 \equiv 123.226^{221} \ mod\ 233$

$\boldsymbol{c30 \equiv 74}$

$c31 \equiv 100.26^{233-1-11} \ mod\ 233$

$c31 \equiv 100.26^{221} \ mod\ 233$

$\boldsymbol{c31 \equiv 142}$

$c32 \equiv 157.109^{233-1-11} \ mod\ 233$

$c32 \equiv 157.109^{221} \ mod\ 233$

$\boldsymbol{c32 \equiv 26}$

$c33 \equiv 227.129^{233-1-11} \ mod\ 233$

$c33 \equiv 227.129^{221} \ mod\ 233$

$\boldsymbol{c33 \equiv 84}$

$c34 \equiv 72.202^{233-1-11} \ mod\ 233$

$c34 \equiv 72.202^{221} \ mod\ 233$

$\boldsymbol{c34 \equiv 231}$

$c35 \equiv 229.62^{233-1-11} \ mod\ 233$

$c35 \equiv 229.62^{221} \ mod\ 233$

$\boldsymbol{c35 \equiv 205}$

$c36 \equiv 89.178^{233-1-11} \ mod\ 233$

$c36 \equiv 89.178^{221} \ mod\ 233$

$\boldsymbol{c36 \equiv 214}$

$c37 \equiv 45.60^{233-1-11} \ mod\ 233$

$c37 \equiv 45.60^{221} \ mod\ 233$

$\boldsymbol{c37 \equiv 10}$

$c38 \equiv 197.200^{233-1-11} \ mod\ 233$

$c38 \equiv 197.200^{221} \ mod\ 233$

$\boldsymbol{c38 \equiv 16}$

$c39 \equiv 173.220^{233-1-11} \ mod\ 233$

$c39 \equiv 173.220^{221} \ mod\ 233$

$\boldsymbol{c39 \equiv 159}$

$c40 \equiv 187.109^{233-1-11} \ mod\ 233$

$c40 \equiv 187.109^{221} \ mod\ 233$

$\boldsymbol{c40 \equiv 60}$

$c41 \equiv 29.14^{233-1-11} \ mod\ 233$

$c41 \equiv 29.14^{221} \ mod\ 233$

$\boldsymbol{c41 \equiv 36}$

$c42 \equiv 44.26^{233-1-11} \ mod\ 233$

$c42 \equiv 44.26^{221} \ mod\ 233$

$\boldsymbol{c42 \equiv 165}$

$c43 \equiv 97.181^{233-1-11} \ mod\ 233$

$c43 \equiv 97.181^{221} \ mod\ 233$

$\boldsymbol{c43 \equiv 245}$

$c44 \equiv 155.66^{233-1-11} \ mod\ 233$

$c44 \equiv 155.66^{221} \ mod\ 233$

$\boldsymbol{c44 \equiv 118}$

$c45 \equiv 119.167^{233-1-11} \ mod\ 233$

$c45 \equiv 119.167^{221} \ mod\ 233$

$\boldsymbol{c45 \equiv 186}$

$c46 \equiv 178.50^{233-1-11} \ mod\ 233$

$c46 \equiv 178.50^{221} \ mod\ 233$

$\boldsymbol{c46 \equiv 234}$

$c47 \equiv 179.30^{233-1-11} \ mod\ 233$

$c47 \equiv 179.30^{221} \ mod\ 233$

$\boldsymbol{c47 \equiv 122}$

$c48 \equiv 112.133^{233-1-11} \ mod\ 233$

$c48 \equiv 112.133^{221} \ mod\ 233$

$\boldsymbol{c48 \equiv 245}$

$c49 \equiv 67.101^{233-1-11} \ mod\ 233$

$c49 \equiv 67.101^{221} \ mod\ 233$

$\boldsymbol{c49 \equiv 20}$

Setelah mendapatkan nilai mn, masing-masing nilai m hasil dari dekripsi menjadi kode ASCII diubah kembali menjadi bilangan ascii heksadesimal (plainteks). Dengan hasil sebagai berikut :

Tabel 5. *Konversi Plainteks ASCII Ke Bilangan Heksadesimal*

No	Plainteks Kode ASCII	Bilangan Heksadesimal
1	8	08
2	39	27
3	251	FB
4	38	26
5	207	CF
6	25	19
7	71	47
8	254	FE
9	75	4B
10	175	AF
11	98	62
12	253	FD
13	149	95
14	191	BF
15	203	CB
16	194	C2
17	205	CD
18	225	E1
19	182	B6
20	241	F1
21	50	32
22	220	DC
23	204	CC
24	97	61
25	230	E6
26	230	E6
27	105	69
28	54	36
29	143	8F
30	74	4A
31	142	8E
32	26	1A
33	84	54
34	231	E7
35	205	CD
36	214	D6
37	10	0A
38	16	10
39	159	9F
40	60	3C
41	36	24
42	165	A5
43	245	F5
44	118	76
45	186	BA
46	234	EA
47	122	7A
48	245	F5
49	20	14

Hasil plaintext setelah didekripsi, seperti sampel gambar berikut ini:

Gambar 5. *Hasil Plainteks setelah gambar didekripsi*

PEMBAHASAN

Pada penelitian ini sistem yang akan dibangun menggunakan Visual Basic. Net 2010, antarmuka pada aplikasi yang dikembangkan dapat dilihat pada gambar dibawah ini :

Form Menu Utama

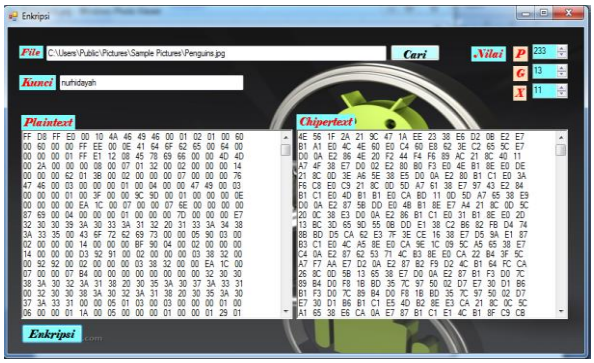
Dibawah ini adalah tampilan form menu utama :

Gambar 6. *Form Utama*

Form ini merupakan tampilan awal program untuk memilih beberapa pilihan menu pada sistem.

Fom Enkripsi

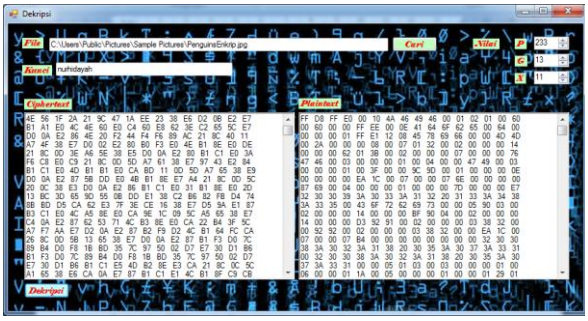
Pada proses ini adalah cara mengenkrip file gambar, dengan menekan tombol cari untuk file gambar yang akan dienkripsi, lalu masukan nilai p, g, x, serta masukan kunci, setelah itu pilih tombol enkripsi seperti gambar di bawah ini :



Gambar 7. *Proses Enkripsi File Gambar*

Form Dekripsi

Pada proses ini cara mendekrip (mengembalikan ke gambar aslinya), dengan menekan tombol cari untuk file gambar yang akan didekripsi, lalu masukan nilai p, g, x, serta masukan kunci, setelah itu pilih tombol dekripsi seperti gambar di bawah ini :



Gambar 8. *Proses Dekripsi File Gambar*

KESIMPULAN

Berdasarkan penelitian yang dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Teknik yang dilakukan dalam pengamanan file gambar yaitu dengan cara menerapkan algoritma elgamal kedalam aplikasi ini yang dapat mengubah file asli kedalam file rahasia.
2. Dari hasil percobaan yang dilakukan aplikasi ini dapat mengenkrip file dengan baik dan menutup kecurigaan dari pihak lain. Pada proses dekripsi dapat mengembalikan file yang dienkripsi dengan baik dan tidak merusak file aslinya.
3. Penggunaan kunci p, g, x dalam algoritma elgamal merupakan sesuatu yang sangat penting dalam proses enkripsi dan dekripsi, sehingga dibutuhkan suatu kerahasiaan dalam pemakaian kunci.

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran yang dapat digunakan sebagai masukan untuk penelitian selanjutnya antara lain :

1. Input untuk proses enkripsi tidak hanya dilakukan untuk format berbentuk *jpg saja, akan tetapi bisa juga digunakan untuk mengenkripsi file gambar yang berformat *png, *bmp dan *gif.
2. Aplikasi ini diharapkan dapat dikembangkan kedalam proses jaringan internet oleh penulis-penulis selanjutnya.
3. Untuk pengembangan lebih lanjut diharapkan dapat menambahkan sistem keamanan yang lebih baik lagi pada perangkat lunak ini.
4. Aplikasi ini diharapkan dapat dikembangkan dengan metode-metode yang lainnya sebagai perbandingan dan menjadi sistem yang lebih mendekati kepada keperawatan serta solusi yang lebih baik.

DAFTAR PUSTAKA

[1]Kromodimoeljo, Sentot 2009. Teori dan Aplikasi Kriptografi. Penerbit SPK IT Consulting.

[2]Ariyus, Dony 2008. *Computer Security*. Penerbit Andi. Yogyakarta

[3] Pardede, A. M. H., & Maulita, Y. (2014). PERANCANGAN PERANGKAT LUNAK ENKRIPSI DAN DESKRIPSI FILE DENGAN METODE TRANSPOSISI KOLOM. *KAPUTAMA*, *8*(1), 28–35.

[4] Pardede, A. M. H. (2017). Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen. *Jurnal Teknik Informatika Kaputama (JTIK)*, *1*(1).

[5]Ariyus, Dony 2006. Kriptografi Keamanan Data Dan Komunikasi**.** Penerbit Graha Ilmu. Tanggerang