IMPLEMENTASI KRIPTOGRAFI KUNCI ASIMETRI EL-GAMAL UNTUK KERAHASIAAN DATA CITRA DIGITAL

Esti Suryani
Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sebelas Maret, Surakarta 57126
E-mail : suryapalapa@yahoo.com

ABSTRAK

Jaringan komunikasi seperti internet adalah jaringan yang tidak aman untuk transmisi data, seperti teks, audio, maupun citra digital. Salah satu cara untuk mengamankan data tersebut yaitu dengan enkripsi,. Tujuannya adalah untuk kerahasiaan data. Penelitian ini menggunakan metode kriptografi kunci asimetrik dengan algoritma El-Gamal yang diterapkan untuk pesan berupa citra digital. Citra yang digunakan dalam penelitian ini adalah citra grayscale. Proses enkripsi dan dekripsi terhadap citra digital menggunakan satu pasangan kunci. Kunci yang digunakan untuk enkripsi disebut kunci publik, sedangkan kunci yang dipakai untuk dekripsi disebut kunci privat. Membuktikan ada atau tidaknya kesalahan antara plain image (citra semula sebelum dieknripsi) dan decipher image (citra hasil dekripsi dari citra yang telah dienkripsi) digunakan metode Root Mean Square Error (rmse). Hasil yang diperoleh berupa citra yang telah dapat dilakukan proses enkripsi untuk tujuan kerahasiaan dalam proses pengiriman, dan citra hasil dekripsi untuk mengetahui pesan semula yang berupa citra tersebut. Proses enkripsi dan dekripsi pada kriptosistem El-Gamal ini berhasil jika salah satu kunci publik yaitu bilangan prima yang diinputkan minimal 257.

Kata kunci : enkripsi, publik, private, El-Gamal, cipher, decipher

1. PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Kemajuan yang cepat pada teknologi jaringan digital, keamanan multimedia menjadi lebih penting, saat data lebih sering ditransmisikan pada jaringan yang terbuka. Salah satu hal yang penting dalam hal komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin keamanan pesan, data, ataupun informasi berupa citra digital yaitu dengan menggunakan implementasi teknik kriptografi. Paper ini akan difokuskan pada pengamanan pesan berupa file citra digital *grayscale* dengan algoritma kriptografi kunci asimetrik El-Gamal.

2. KRIPTOGRAFI

Kriptografi: adalah seni dan ilmu untuk menulis rahasia *"The Art of Secreet Wraiting"*. Tujuannya agar pesan tidak dapat dibaca. Proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext)* menjadi pesan yang tersembunyi *(ciphertext)* disebut dengan **enkripsi** *(encryption)*. *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Proses sebaliknya untuk mengubah *ciphertext* menjadi *plaintext*, disebut **dekripsi** *(decryption)*.

2.1 Kriptografi Kunci Simetri

Kunci simetris adalah metode kriptografi yang sering digunakan. Kunci yang dipakai untuk membuat pesan yang disandikan sama dengan kunci yang dipakai untuk membuka pesan yang disandikan. Jadi pihak pengirim dan penerima harus memiliki kunci yang sama, yaitu kunci enkripsi sama dengan kunci dekripsi, dengan algoritma yang kuat, keamanan pesan tergantung pada kerahasiaan kunci. Sebuah kriptosistem mempunyai lima komponen *(P,C,K,E,D)*, dimana memenuhi kondisi di sebagai berikut [1]:

1. *P* adalah himpunan berhingga plaintext
2. *C* adalah himpunan berhingga ciphertext
3. *K* adalah ruang kunci, merupakan himpunan berhingga
4. Untuk setiap $k \in K$, terdapat suatu aturan enkripsi $e_k \in E$ dan bersesuaian dengan aturan dekripsi $d_k \in D$. Setiap $e_k : P \to C$ dan $d_k : C \to P$ semuanya merupakan fungsi-fungsi, yaitu $d_k(e_k(x)) = x$ untuk setiap plaintext $x \in P$.

2.2 Kriptografi Kunci Asimetrik

Kriptografi kunci asimetrik disebut juga kriptografi kunci publik, pertama kali dipublikasikan oleh Diffie dan Hellman pada tahun 1976. Kriptografi kunci publik merupakan kriptografi dengan kunci asimetri, menggunakan dua buah kunci, berbeda dengan kunci simetri yang hanya menggunakan satu kunci [2]. Kunci publik dan kunci privat merupakan pasangan kunci, dimana kunci publik merupakan kunci untuk mengenkripsi pesan, dan kunci privat merupakan kunci untuk mendekripsi pesan, pasangan kunci ini dibuat oleh penerima. Kunci publik semua orang boleh mengetahui sedangkan kunci privat hanya penerima saja yang mengetahuinya. Kunci publik dan kunci privat merupakan pasangan kunci, dimana kunci publik merupakan kunci untuk mengenkrip pesan, dan kunci privat merupakan kunci untuk mendekrip. Kunci publik semua orang boleh mengetahui sedangkan kunci privat hanya penerima saja yang mengetahuinya. Skema enkripsi dan dekripsi dari sistem kunci publik adalah sebagai berikut :

- Pesan (disebut plaintext) dari A, akan dienkripsi dengan kunci publik milik B.
- Setelah pesan yang dienkrip (disebut ciphertext) sampai pada B, ciphertext ini kemudian didekripsi dengan kunci privat milik B, sehingga B sebagai penerima dapat membaca plaintext yang dikirim oleh A.

2.3 Kunci Asimetrik El-Gamal

Kriptosistem dengan kunci asimetrik El-Gamal berdasarkan pada logaritma diskrit *(Discrete Logarthm)* [1]. Algoritma El-Gamal ini didasarkan pada masalah bilangan bulat modulo *n* dinotasikan dengan Z_n, khususnya *n* adalah prima, dinotasikan dengan Z_p yaitu bilangan bulat modulo bilangan prima, dimana *p* adalah prima, (mengingat kembali group perkalian *(multiplicative group)* Z_p^* adalah *cyclic* dan pembangkit *(generator)* Z_p^* disebut *primitive element*.

2.3.1 Enkripsi dengan Kunci Publik El-Gamal

Pengirim A mengenkripsi pesan *plaintext m* untuk B, dimana B akan mendekripsi pesan yang telah berupa *ciphertext*.
Hal-hal yang dilakukan oleh A adalah sebagai berikut :

a. A telah menerima kunci publik $kp_B = (p, \alpha, \beta)$ dari B dimana $\beta = \alpha^a \bmod p$
b. Merepresentasikan pesan *m* ke dalam bilangan bulat dengan range {0,1,...,*p*-1}
c. Memilih secara random bilangan bulat *k*, $0 \le k \le p-2$
d. Menghitung $\gamma = \alpha^k \bmod p$ dan $L = \beta^k \bmod p$
e. Mengenkripsi pesan $\delta = (m.L) \bmod p$
f. A mengirimkan $c = (\gamma, \delta)$ ke B

2.3.2 Dekripsi dengan Kunci Privat El-Gamal

B sebagai penerima pesan yang berupa *ciphertext* akan mendekripsi *ciphertext* untuk memperoleh pesan semula. B akan melakukan hal-hal berikut :

a. B telah menerima *ciphertext* dari A, yaitu $c = (\gamma, \delta)$, dimana $\gamma = \alpha^k \bmod p$ dan $\delta = (m.L) \bmod p$
b. Dengan kunci privat $kr_B = a$ dihitung $D = \gamma^a \bmod p$ kemudian menentukan inversnya yaitu $D^{-1} = (\gamma^a)^{-1} \bmod p$
c. Selanjutnya menentukan kembali *plaintextnya* disebut juga *deciphertext:*

$$m = (\delta . D^{-1}) \bmod p$$

3. CITRA DIGITAL

Citra digital merupakan suatu matriks yang terdiri dari baris dan kolom, dimana setiap pasangan indeks baris dan kolom menyatakan suatu titik pada citra. Nilai matriksnya menyatakan nilai kecerahan titik tersebut. Titik-titik tersebut dinamakan sebagai elemen citra, atau *pixel (picture elemen)*[3].
Andaikan citra kontinyu *f(x,y)* dinyatakan dengan bentuk array *N* x *M*, dimana setiap elemen array adalah nilai diskrit, ditunjukkan dalam persamaan (1) sebagai berikut [3]:

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & f(1,1) & \dots & f(1,M-1) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,M-1) \end{bmatrix} \quad (1)$$

Indeks baris *(i)* dan indeks kolom *(j)* menyatakan koordinat titik pada citra, sedangkan *f(i,j)* merupakan intensitas (derajad keabuan) pada titik *(i,j)*. Setiap elemen pada citra digital (elemen matriks) disebut *image element*, *picture element* atau *pixel* atau *pel*, atau dalam bahasa Indonesia ditulis piksel. Jadi, citra dengan ukuran *N* x *M* mempunyai *NM* buah piksel.

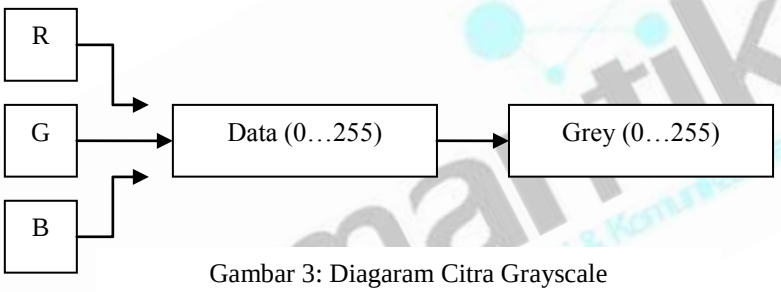
3.1 Citra *Grayscale*

Citra *gray* disebut juga citra abu-abu. Intensitas *f* dari citra hitam putih pada titik *(x,y)* disebut derajad keabuan *(gray level)*, dalam hal ini derajad keabuan dari hitam ke putih, citra disebut citra hitam putih *(grayscale image)*. Derajad keabuan memiliki rentang nilai dari :

$$L_{\min} < f < L_{\max} \quad (2)$$

dimana selang antara $(L_{\min}, L_{\max})$ disebut skala keabuan. Selang $(L_{\min}, L_{\max})$ untuk alasan praktis menjadi selang $[0, L]$, nilai intensitas 0 menyatakan hitam, dan nilai intensitas *L* menyatakan putih, sedangkan nilai intensitas antara 0 sampai *L* bergeser dari hitam ke putih, [3].

Pada citra *grayscale* (8 bit) nilai warna primer (merah, hijau, biru) mempunyai nilai yang sama yaitu antara 0-255. Citra *gray* merupakan citra dua dimensi (2D), yang direpresentasikan ke dalam sebuah matriks 2D. Posisi baris dan kolom pada matriks menunjukkan posisi piksel pada citra, sedangkan warna piksel adalah nilai yang tersimpan dalam citra. Di bawah ini adalah skema citra *grayscale* yang mana nilai R,G, B mempunyai nilai yang sama. Maksudnya nilai komponen tiga warna dasar (R,G,B) pada (*x*,*y*) mempunyai nilai yang sama.



Gambar 3: Diagaram Citra Grayscale

3.2 Kesamaan Citra Digital

Salah satu metode untuk mengetahui sama atau tidaknya antara satu citra dengan citra yang lain adalah dengan cara membandingkan antara citra yang satu dengan citra yang lain. Misalkan terdapat citra A dan citra B, akan dicocokkan apakah citra A itu sama atau tidak dengan citra B. Salah satu metode yang dapat dipakai untuk mengetahui sama tidaknya citra A dan citra B yaitu dengan metode *Root Mean Square Error* (e_{rms}). Untuk masing-masing citra berukuran M x N, e_{rms} dapat dirumuskan sebagai berikut,[3] :

$$e_{rms} = \left[\frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{n-1} \left(f_B(x,y) - f_A(x,y) \right)^2 \right]^{\frac{1}{2}} \quad (3)$$

dengan $f_A(x,y)$ adalah nilai intensitas pixel citra A, dan $f_B(x,y)$ adalah nilai intensitas pixel citra B.

Nilai e_{rms} menentukan sama tidaknya sebuah citra digital secara significant. Jika e_{rms} bernilai nol maka kedua citra tersebut identik sama.

4. ALGORITMA UNTUK IMPLEMENTASI PERANCANGAN SISTEM

Implementasikan perancangan sistem kriptografi kunci asimetrik El-Gamal tersebut, diperlukan algoritma-algoritma yang dipakai untuk sistem kriptografi yang akan dibuat, yaitu sebagai berikut :

4.1 Algoritma Menggenerate Kunci

Bagian ini dalam konsep user B sebagai penerima menggenerate pasangan kunci, yaitu kunci publik yang akan digunakan sebagai kunci enkripsi, dan kunci privat yang akan digunakan untuk dekripsi, user mengerjakan hal-hal berikut ini :

1) Generate bilangan prima p dengan algoritma (1) , bilangan prima diinputkan, dan generator α dari group perkalian Z_p^* bilangan bulat modulo p (menggunakan algoritma (2)).
2) Pilih secara random bilangan bulat a, $1 \le a \le p-2$, dan menghitung $\beta = \alpha^a \bmod p$ dengan algoritma (3.3)
3) Kunci publiknya adalah (p, α, β), kunci privatnya adalah a

4.1.1 Menggenerate bilangan prima *p* dan generator α dari Z_p^*, yaitu group perkalian bilangan bulat modulo *p*

Untuk menggenerate bilangan prima p, (menggunakan algoritma (1), berikut ini :

- **Algoritma (1)**

Algoritma menentukan bilangan prima *p* :

Input : bilangan bulat positif
Output : Bilangan prima atau bukan bilangan prima
1. Input bil
2. Ket = 'prima'
3. if bil = 2 then Ket = 'prima'
4. Else if (bil mod 2 0) then Ket = 'bukan prima'
5. Else
    5.1 batas = sgrt (bil) + 1
    5.2 pembagi = 3
    5.4 While (pembagi < = batas) do
        5.4.1 If (bil mod pembagi = 0) then Ket = 'bukan prima'
        5.4.2 pembagi = pembagi + 2 ;
6. Hasil (bil) adalah (Ket).

4.1.2 Memilih secara random bilangan bulat α , $1 \le a \le p-2$, dan menghitung $\alpha^a \bmod p$

Algoritma untuk memilih secara random bilangan bulat a, $1 \le a \le p-2$, dan menghitung $\beta = \alpha^a \bmod p$ adalah pada dasarnya menggunakan algoritma pemangkatan (3), berikut ini :

- **Algoritma 3**

Input : $\alpha \in Z_p^*$, dan bilangan bulat $1 \le a < p-2$ yang mana direpresentasikan secara biner (dikonversi dari desimal ke biner) yaitu $a = \sum_{i=0}^{t-1} k_i 2^i$

Output : $\beta = \alpha^a \bmod p$

1. Set $\beta \leftarrow 1$. If $k_0 = 0$ hasil β
2. Set $A \leftarrow \alpha$
3. If $k_0 = 1$ then $\beta \leftarrow \alpha$
4. For $i = 1$ to $t-1$ do (*mulai indeks* $i = 0$ *sampai* $i = t-1$ *adalah digit biner a)*
    4.1.1 Set $A \leftarrow A^2 \bmod p$
    4.1.2 If $k_i = 1$ then $\beta \leftarrow A \cdot b \bmod p$
5. Hasil (β).

4.2 Algoritma untuk Implementasi Enkripsi

Pembuatan kriptosistem citra digital dengan kunci asimetrik El-Gamal ini data-data yang dipakai sebagai percobaan adalah file citra digital berformat BMP, dengan intensitas nilai piksel antara 0 sampai 255.

4.2.1 Algoritma Enkripsi Citra *Grayscale*

Proses enkripsi *plain image* berformat BMP. Citra dienkripsi dengan kunci publik (k_p), citra yang diinputkan (*plain image*) merupakan citra *grayscale* berukuran NxM dimana N adalah panjang dan M adalah lebarnya.
Langkah-langkah proses enkripsi file *image grayscale* adalah sebagai berikut :

a. Citra tersebut dibaca sebagai matrik berukuran NxM yang akan dibaca piksel per piksel mulai dari posisi piksel (0,0), (0,1)….sampai posisi (N-1,M-1). Sedangkan nilai dari piksel-piksel tersebut adalah *f(x,y)* dimana $\{ f(x,y) \mid 0 \le x \le 255$ dan $0 \le y \le 255 \}$.

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & & f(0,M-1) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ f(N-1,0) & \dots & \dots & f(N-1,M-1) \end{bmatrix}$$

Nilai dari $\{ f(x,y) \mid 0 \le x \le 255$ dan $0 \le y \le 255\}$ dimana nilai *f(x,y)* merupakan intensitas *grayscale* dikonversi menjadi integer.

b. Setiap nilai piksel $\{ f(x,y) \mid 0 \le x \le 255$ dan $0 \le y \le 255\}$ merupakan pesan yang akan dienkripsi.

c. Dengan kunci publik El-Gamal $kp_B = \{p, \alpha, \beta)$ yang secara konsep telah digenerate oleh B sebagai penerima dan telah diterima oleh A sebagai pengirim, A akan dilakukan proses enkripsi .

d. Kunci publik dan kunci privat telah digenerate adalah sebagai berikut :

- kunci publik $kp_B = \{p, \alpha, \beta)$; $\beta = \alpha^a \bmod p$ dan kunci privat $kr_B = a$, *p* adalah bilangan prima, *a* random bilangan bulat $1 \le a \le p-2$, α adalah generator $Z_p{}^*$ group perkalian bilangan bulat modulo *p*.
- Bilangan prima yang digunakan di nilainya di atas 255 karena pesan direpresentasikan antara 0 sampai p-1

e. Telah diperoleh bilangan prima *p*, generator $\alpha \in Z_p^*$, $\beta = \alpha^a \bmod p$

f. Memilih random bilangan bulat *k* , dimana $1 \le k \le p-2$

g. Menghitung $\gamma = \alpha^k \bmod p$ *(dengan algoritma 4)* berikut ini :

Algoritma 4

Menghitung $\gamma = \alpha^k \bmod p$

Input : Generator $\alpha \in Z_p^*$, bilangan prima *p,* dan random bilangan bulat *k*, dimana $1 \le k \le p-2$, *k* direpresentasikan ke dalam biner $k = \sum_{i=0}^{t-1} k_i 2^i$

Output : $\gamma = \alpha^k \bmod p$

1. Set $\gamma \leftarrow 1$, if $k_0 = 0$ then hasil γ
2. Set $A \leftarrow \alpha$
3. If $k_0 = 1$ then $\gamma \leftarrow \alpha$
4. For $i = 1$ to $t-1$ (digit biner *k* dimulai dari index $i = 0$ sampai $i = t-1$)
   4.1 Set $A \leftarrow A^2 \bmod p$
   4.2 If $k_i = 1$ then $\gamma \leftarrow A.\gamma \bmod p$
5. Hasil (γ)

h. Menghitung $L = \beta^k \bmod p$ *(dengan algoritma 5)*

Algoritma 5

Menghitung $L = \beta^k \bmod p$

Input : $\beta \in Z_p^*$, bilangan prima *p,* dan random bilangan bulat *k*, dimana $1 \le k \le p-2$, *k* direpresentasikan ke dalam biner $k = \sum_{i=0}^{t-1} k_i 2^i$

Output : $L = \beta^k \bmod p$

1. Set $L \leftarrow 1$ if $k_0 = 0$ then hasil *L*
2. Set $A \leftarrow \beta$
3. If $k_0 = 1$ then $L \leftarrow \beta$
4. For $i = 0$ to $t-1$ do
   4.1 Set $A \leftarrow A^2 \bmod p$
   4.2 If $k_i = 1$ then $L \leftarrow A.L \bmod p$
5. Hasil (L)

i. Mengenkripsi *image grayscale* diambil piksel-per piksel $\{ f(x,y) \mid 0 \le x \le 255$ dan $0 \le y \le 255\}$;

$$f'(x,y) = (f(x,y) \times L) \bmod p$$

j. A mengririmkan $(\gamma, f'(x,y))$ kepada B

4.3 Algoritma untuk Implementasi Dekripsi

4.3.1 Algoritma untuk Dekripsi Citra *Grayscale*

Proses enkripsi citra *grayscale* yang telah disebutkan sebelumnya telah diperoleh *cipher image* $\{ f'(x,y) \mid 0 \le x \le 255$ dan $0 \le y \le 255 \}$.

$$f'(x,y)\begin{bmatrix} f'(0,0) & f'(0,1) & & f'(0,M-1) \\ f'(1,0) & \dots & \dots & f'(1,M-1) \\ \dots & \dots & \dots & \dots \\ f'(N-1,0) & \dots & \dots & f'(N-1,M-1) \end{bmatrix}$$

Cipher image $f'(x,y)$ tersebut akan didekripsi untuk memeperoleh kembali *plain image* atau disebut *decipher image*. Urutan langkah dekripsi *cipher image* dapat ditunjukkan sebagai berikut :

a. Telah dihitung pada desain enkripsi sebelumya bahwa B telah menerima $\gamma = \alpha^k \bmod p$ dan *cipher image gray scale* $\{ f'(x,y) = (f(x,y) \times L) \bmod p \mid$ dan untuk memperoleh kembali *plain image* atau *decipher imege* selanjutnya yang harus dilakukan adalah :

b. Kunci privat $kr_B = a$

c. Menghitung $D = \gamma^a \bmod p$ *dengan algoritma 6* berikut ini :

Algoritma 6

Menghitung $D = \gamma^a \bmod p$

Input : $\gamma \in Z_p^*$, bilangan prima *p*, dan random bilangan bulat *a*, dimana $1 \le a \le p-2$, *k* direpresentasikan ke dalam biner $a = \sum_{i=0}^{t-1} a_i 2^i$

Output : $D = \gamma^a \bmod p$

1. Set $D \leftarrow 1$ if $a_0 = 0$ then hasil *D*
2. Set $A \leftarrow \gamma$
3. If $a_0 = 1$ then $D \leftarrow \gamma$
4. For $i = 1$ to $t-1$ do
   4.1 Set $A \leftarrow A^2 \bmod p$
   4.2 If $a_i = 1$ then $D \leftarrow A.D \bmod p$
5. Hasil (*D*)

d. Menghitung inversnya yaitu $D^{-1} = I$ merupakan invers dari $D = \gamma^a \bmod p$ *(dengan algoritma 7 berikut ini):*

Algoritma 7

Algoritma untuk menghitung invers Z_p^* , Group perkalian modulo *p* dimana *p* adalah prima

Input : $D \in Z_p^*$ dan $p \in Z_p^*$

Output : $I = D^{-1}$ dimana output dapat dirpresentasikan sebagai berikut

menentukan *x*dan *y* yang memenuhi $Dx + py = d$ dimana $d = \gcd(D, p)$ sedemikian sehingga $d = 1$

1. If $p = 0$ then

set $d \leftarrow D,\ x \leftarrow 1,\ y \leftarrow 0$, dan hasil (d, x), *dimana x adalah inversnya*

2. Set $x_2 \leftarrow 1,\ x_1 \leftarrow 0,\ y_2 \leftarrow 0\ ,\ y_1 \leftarrow 1$
3. While $p > 0$ do

$q \leftarrow \lfloor D / p \rfloor$, *q dibulatkan ke bawah*

$r \leftarrow D - qn, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1, D \leftarrow p, p \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x$

$y_2 \leftarrow y_1, y_1 \leftarrow y$

4. Set $d \leftarrow D,\ x \leftarrow x_2,\ y \leftarrow y_2$
5. If $d > 1$, then D^{-1} tidak ada *(tidak ada invernya)*, selainnya hasil (*d*,*x*), dimana *x* adalah invernya.

e. Mendekrip *cipher image grayscale* $f(x,y) = (f'(x,y) \times D^{-1}) \bmod p$

f. Diperoleh *decipher image* atau *plain image* semula.

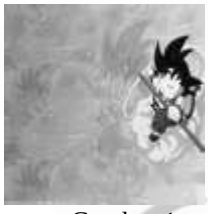
5. HASIL DAN PEMBAHASAN

Berikut ini ditunjukkan hasil pengujian enkripsi dan dekripsi terhadap citra *grayscale DragonBall*, dengan memvariasikan pasangan kunci seperti ditunjukkan pada gambar di atas. Kunci-kunci tersebut digunakan untuk proses enkripsi dan dekripsi dengan file citra *grayscale* dengan ukuran yang sama, yang hasilnya dapat ditunjukkan pada tabel :

Tabel 1 : Enkripsi Dekripsi Citra *Grayscale* Ukuran Citra sama dengan Kunci Berbeda

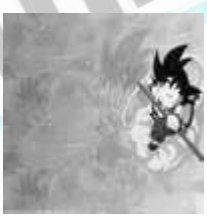
Grayscale Nama File : DragonBall Size :100x100					
Enkripsi			Dekripsi		Error Relatif
Kunci Publik	Proses	Waktu Milidetik	Kunci Private	Proses	
publik4.pub $p = 257$ $\alpha = 31$ $\beta = 198$	$k = 221$ $\gamma = 244$ $L = 29$	31	**private4.priv** $a = 19$	$D = 29$ $D^{-1} = 62$	0
contoh2.pub $p = 127$ $\alpha = 95$ $\beta = 119$	$k = 102$ $\gamma = 64$ $L = 32$	16	**contoh2.priv** $a = 37$	$D = 32$ $D^{-1} = 4$	134.275

Contoh hasil enkripsi dengan kunci **publik4.pup** dan dekripsi dengan kunci **privat4.priv** (tabel 1 di atas) pada citra grayscale Dragon Ball ukuran 100 x 100, ditunjukan pada gambar 1(a,b,c) berikut ini:



Gambar 1a:
Plain Image,
DragonBall_100x100

Gambar 1b:
Plain Image,
DragonBall_100x100



Gambar 1c:
Plain Image,
DragonBall_100x100

Contoh hasil enkripsi dengan kunci **contoh2.pup** dan dekripsi dengan kunci **contoh2.priv** (tabel 1 di atas) pada citra grayscale Dragon Ball ukuran 100 x 100, ditunjukan pada gambar 2 (a,b,c) berikut ini:

Gambar 2a:
Plain Image,
DragonBall_100x100

Gambar 2b:
Cipher Image,
DragonBall_100x100

Gambar 2c:
Decipher Image,
DragonBall_100x100

5. PENUTUP

Kerahasiaan pesan citra digital dengan kriptografi kunci asimetri El-Gamal telah dapat diimplementasikan, input bilangan prima antara 0-255, *cipher image* tidak dapat didekripsi dengan baik, karena bilangan prima yang diinputkan masih di dalam range pesan yang berupa piksel citra digital yang mempunyai range 0-255,

karena dalam algoritma El-Gamal pesan direpresentasikan antara $(0,\ldots\ldots,p-1)$, jadi input bilangan prima yang dapat memenuhinya minimal adalah 257.

DAFTAR PUSTAKA

[1] Gonzalez, R.C., Woods, R.E., 1992, *Digital Image Processing*, Addison-Wesley Publishing Company, USA.
[2] Menezes, A., Van Oorschot, P., and Vanstone,S., 1996, *Handbook of Applied Cryptography*, CRC Press Boca Roton.
[3] Stallings, William., 1995, *Network and Internetwork Security Principles and Practice*, Prentice Hall, Englewood Cliffs, New Jersey 0763
[4] Stallings, William., 2000, *Network Security Essentials : Applications and Standards*, Prentice Hall, Upper Saddle River, New Jersey 07458
[5] Stinson, Douglas R., 1995, *Cryptography Theory and Practice*, CRC Pres Boca Raton London Tokyo
[6] Burton, David.M, 1998, *Elementary Number Theory*, The McGraw-Hill Companies, Inc.
[7] Droogenbroeck, Marsc Van., *Partial Encryption of Image For Real-Time Applications*, Institut Montefiore B-28, Departement of Electricity, Electronics and Computer Science, Sart Tilman, B-4000 Liege, Belgium.