Penerapan Algoritma Kriptografi ElGamal untuk Pengaman File Citra

M. Taufiq Tamam[1], Wakhyu Dwiono[2], Tri Hartanto[3]

***Abstract* - Application security system image file is created in this research using ElGamal cryptographic algorithms and compiler program used is Borland Delphi 7. ElGamal cryptography algorithm is one of the key asymmetric cryptographic algorithm that uses a different key pair, an encryption key and a decryption key. Results from these applications can encrypt a bitmap image file type with 24-bit pixel format. Image generated using the extension "Este".**

***Key word:* image, cryptography, ElGamal, bitmap, este**

***Abstrak* - Aplikasi sistem keamanan file citra yang dibuat pada penelitian ini menggunakan algoritma kriptografi ElGamal dan compiler program yang digunakan adalah Borland Delphi 7. Algoritma kriptografi ElGamal merupakan salah satu algoritma kriptografi kunci asimetris yang menggunakan sepasang kunci yang berbeda, satu kunci enkripsi dan satu kunci dekripsi. Hasil dari aplikasi ini mampu mengenkripsi file citra tipe bitmap dengan format piksel 24 bit. Citra yang dihasilkan menggunakan ekstensi "Este".**

***Kata kunci*: citra, kriptografi, ElGamal, bitmap, este.**

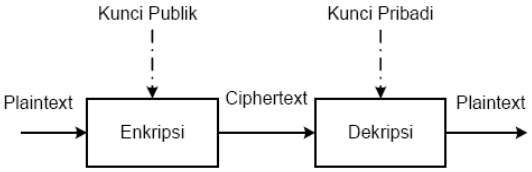
I. PENDAHULUAN

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 di dalamnya. Ilmu kriptografi sebenarnya telah lama digunakan, sejak jaman sebelum mengenal metode pengiriman data menggunakan komputer. Seiring dengan perkembangan teknologi telekomunikasi, maka semakin berkembang pula ilmu kriptografi baik jenis maupun fungsinya.

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 dua buah kunci yaitu kunci publik untuk melakukan enkripsi sedangkan kunci pribadi untuk melakukan dekripsi. Dalam algoritma kunci asimetris, kunci yang didistribusikan adalah kunci publik yang tidak diperlukan kerahasiaanya sedangkan kunci pribadi tetap disimpan atau tidak didistribusikan. Setiap orang yang memiliki kunci publik dapat melakukan proses enkripsi tetapi hasil dari enkripsi tersebut hanya bisa dibaca oleh orang yang memiliki kunci pribadi.

Kajian terdahulu telah dilakukan oleh Irawati yang menghasilkan sebuah program aplikasi enkripsi dan dekripsi menggunakan Algoritma RSA dengan menggunakan *Delphi 7*. Aplikasi tersebut dapat digunakan untuk keamanan data *Text* yang dapat digunakan oleh pemakai program baik secara umum maupun pribadi [4].

Kriptografi kunci publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Kotak surat yang diletakkan di depan rumah pemiliknya sehingga setiap orang dapat memasukkan surat ke dalam kotak tersebut, tetapi hanya pemilik kotak yang dapat membuka dan membaca surat yang ada di dalam kotak tersebut. Kriptografi kunci publik berkembang menjadi sebuah revolusi baru dalam sejarah kriptografi, tidak seperti pada kunci simetris yang hanya didasarkan pada subtitusi dan permutasi saja, akan tetapi kriptografi kunci public didasarkan pada fungsi matematika seperti perpangkatan dan modulus. Konsep kriptografi kunci asimetris dapat dilihat pada Gambar 1.



Gambar 1 Kriptografi kunci asimetris

Algoritma kriptografi ElGamal menggunakan beberapa persamaan untuk melakukan proses *generate key*, proses enkripsi dan proses dekripsi [7].

A. Algoritma Generate Key

Algoritma ElGamal memerlukan sepasang kunci yang dibangkitkan dengan memilih bilangan prima *p* dan dua buah bilangan acak (*random*) *g* dan *x*, dengan syarat bahwa nilai *g* dan *x* lebih kecil dari *p* yang memenuhi persamaan.

$$y = g^x \bmod p \qquad (1)$$

Dari persamaan tersebut nilai *y, g* dan *p* merupakan pasangan kunci public sedangkan *x, p* merupakan pasangan kunci pribadi. Besaran-besaran yang digunakan dalam algoritma kriptografi *Elgamal* adalah:

[1, 2] Staf Pengajar Teknik Elektro UMP Purwokerto (tamamump@yahoo.co.id)
[3] Alumni Teknik Elektro UMP Purwokerto

a. Bilangan prima *p* bersifat tidak rahasia.
b. Bilangan acak *g* (*g* < *p*) bersifat tidak rahasia
c. Bilangan acak *x* (*x* < *p*) bersifat rahasia.
d. Bilangan *y* bersifat tidak rahasia.
e. *m* (*plaintext*) bersifat rahasia merupakan pesan asli yang digunakan untuk data
f. sumber dalam proses enkripsi dan merupakan data hasil pada proses dekripsi.
g. *a* dan *b* (*ciphertext*) bersifat tidak rahasia

B. Algoritma Proses Enkripsi

Algoritma proses enkripsi dilakukan dengan memilih bilangan acak *k* yang berada dalam himpunan $1 \leq k \leq p\text{-}2$. Setiap blok *plaintext m* dienkripsi dengan persamaan

$$a = gk \bmod p \quad (2)$$

$$b = yk\ m \bmod p \quad (3)$$

C. Algoritma Proses Dekripsi

Proses dekripsi menggunakan kunci pribadi *x* dan *p* untuk mendekripsi *a* dan *b* menjadi *plaintext m* dengan persamaan:

$$(ax)^{-1} = a^{p-1-x} \bmod p \quad (4)$$

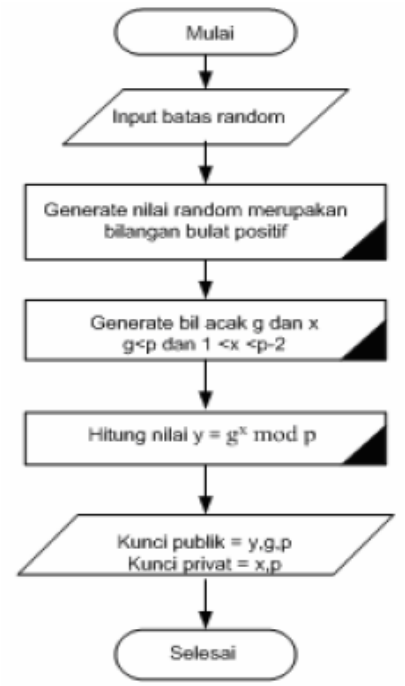
$$m = b * a^{x} \bmod p \quad (5)$$

Sehingga *plaintext* dapat ditemukan kembali dari pasangan *ciphertext a* dan *b*.

II. METODE PENELITIAN

A. *Proses Generate* Key

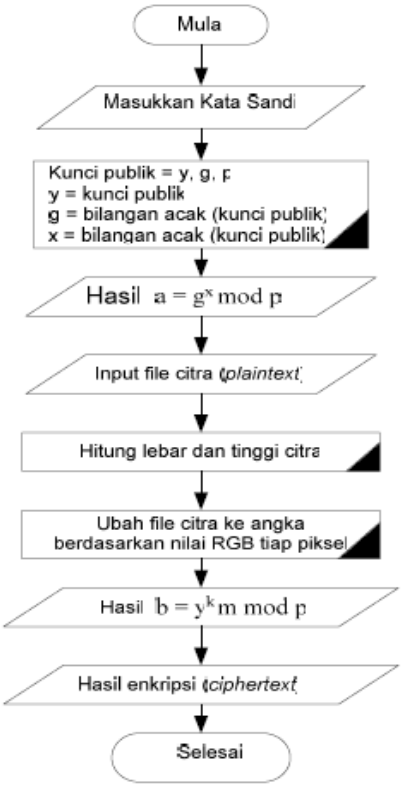
Proses *Generate Key* adalah proses untuk membangkitkan kunci yang digunakan untuk proses enkripsi maupun dekripsi. Rancangan proses *generate key* dapat dilihat pada Gambar 2.



Gambar 2 Diagram alir proses membangkitkan kunci

B. Proses Enkripsi

Proses enkripsi merupakan proses untuk mengubah data sumber menjadi file *ciphertext* dengan menggunakan nilai-nilai kunci publik yang dihasilkan dari proses *generate key*. Rancangan proses enkripsi dapat dilihat pada Gambar 3.



Gambar 3 Diagram alir proses enkripsi

C. Proses Dekripsi

Proses dekripsi adalah proses untuk mengembalikan *ciphertext* kedalam bentuk *plaintext*, dengan menggunakan kunci pribadi (*x*,*p*). Rancangan proses dekripsi dapat dilihat pada Gambar 4.

Gambar 4 Diagram alir proses dekripsi

III. HASIL DAN PEMBAHASAN

A. *Halaman Utama*

Setelah proses perancangan dilakukan maka dihasilkan sebuah aplikasi sistem keamanan data yang siap untuk digunakan. *Form* utama merupakan halaman awal aplikasi kriptografi yang terdiri atas berbagai macam menu yang digunakan untuk membuka halaman-halaman lain yang berkaitan. Tampilan halaman utama aplikasi sistem kriptografi ElGamal dapat dilihat pada Gambar 5.

Gambar 5 Tampilan halaman utama

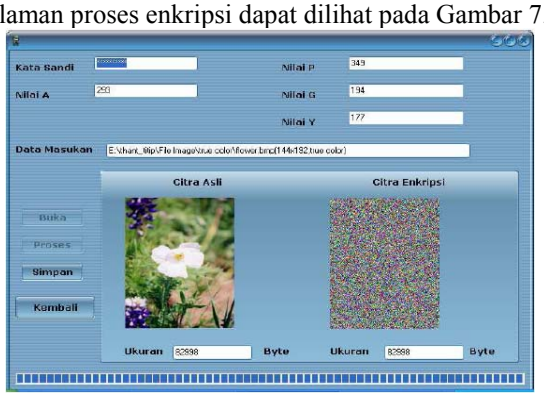
B. *Pembangkitan Kunci*

Langkah awal yang harus dilakukan dalam menggunakan halaman *Generate Key* yaitu dengan memasukkan nilai batas random antara nilai 15 sampai 300. Nilai batas random yang telah dimasukkan tersebut kemudian digunakan untuk membangkitkan nilai prima (*p*), nilai (*g*), nilai (*x*) dengan cara menekan tombol *Enter* pada *keyboard*, selain tombol *Enter* yang ditekan maka perintah tersebut akan diabaikan. Selanjutnya untuk mendapatkan nilai (*y*) cukup dengan menekan menu *Hitung*. Halaman *form Generate Key* dapat dilihat seperti pada Gambar 6.

Gambar 6 Tampilan halaman pembangkitan kunci

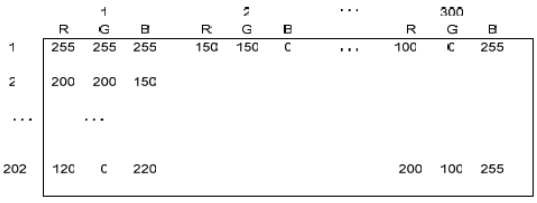
C. *Proses Enkripsi*

Langkah pertama yang harus dilakukan untuk menjalankan proses enkripsi yaitu dengan memasukkan *password*, proses ini dilakukan untuk mengambil nilai kunci publik (*p, g, y*) dari dalam basis data yang merupakan hasil dari proses *generate key*. Langkah selanjutnya yaitu mengambil citra *plaintext* dengan tipe *bitmap*, selanjutnya proses enkripsi dilakukan, ukuran data gambar sebelum maupun sesudah mengalami proses enkripsi dalam satuan *byte* dengan tipe data *Este*. Halaman proses enkripsi dapat dilihat pada Gambar 7.



Gambar 7 Tampilan halaman proses enkripsi

Dengan mengambil contoh suatu file citra yang memiliki format piksel 24bit, maka hasil dari pemrosesan menggunakan program Sistem Kriptografi ElGamal akan dibandingkan dengan hasil pemrosesan dengan cara perhitungan. Berikut ini merupakan hasil analisa dari proses enkripsi yang mengambil nilai masukan yaitu suatu file yang memiliki ukuran luas citra 202x300 dengan asumsi nilai R, G, B seperti pada Gambar 8.



Gambar 8 Ilustrasi nilai RGB pada citra

Nilai tersebut adalah asumsi nilai RGB dari setiap piksel, sehingga diperoleh nilai x dan y misal untuk posisi $f(1,1) = (255\ 255\ 255)$; $f(2,1) = (200\ 200\ 150)$; $f(1,300) = (100\ 0\ 255)$, dengan nilai kunci publik *p*

=317, g =299, y =256, serta bilangan acak k =2. Sehingga dari hasil masukan tersebut dapat dihitung nilai-nilai sebagai berikut.

$$a = g^k \bmod p$$
$$= 299^2 \bmod p$$
$$= 7$$

Blok pesan yang diilustrasikan pada Gambar 8 kemudian dihitung dengan menggunakan rumus $b = y^k m \bmod p$, dengan mengambil salah satu koordinat sebagai contoh yaitu koordinat f(202,300) memiliki intensitas R =200,G =100, B =255.

$$b\,(R) = 256^2 * 200 \bmod 317$$
$$= 65536 * 200 \bmod 317$$
$$= 13107200 \bmod 317$$
$$= 201$$
$$b\,(G) = 256^2 * 100 \bmod 317$$
$$= 65536 * 100 \bmod 317$$
$$= 6553600 \bmod 317$$
$$= 259$$
$$b\,(B) = 256^2 * 255 \bmod 317$$
$$= 65536 * 255 \bmod 317$$
$$= 16711680 \bmod 317$$
$$= 74$$

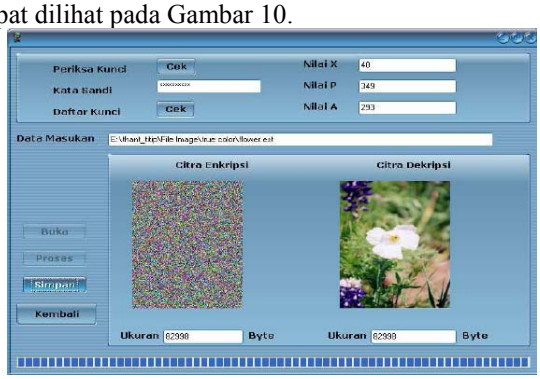
Jadi nilai RGB pada koordinat f (202,300) setelah mengalami proses enkripsi adalah (201, 259, 74), sedangkah nilai a dan b adalah pasangan *ciphertext*. Sehingga dari hasil perhitungan tersebut dapat disusun nilai RGB *ciphertext* seperti Gambar 9.

	1			2			...	300		
	R	G	B	R	G	B	...	R	G	B
1	74	74	74	230	230	0	...	259	0	74
2	201	201	230							
...		...								
202	184	0	126					201	259	74

Gambar 9 Nilai RGB *Ciphertext*

D. *Proses Dekripsi*

Langkah pertama yang harus dilakukan adalah mencari gambar yang akan didekripsi, kemudian memasukkan nilai *x, p, a*. Apabila kita lupa dengan nilai kunci pribadi, maka kita dapat melihatnya pada tabel kunci pribadi dengan cara memasukkan *password* pada kolom daftar kunci. Menu proses akan berfungsi apabila kata kunci yang kita masukkan telah sesuai. Setelah proses dekripsi dilakukan maka akan menghasilkan gambar dengan tipe *bitmap* atau sesuai dengan data sebelum dilakukan proses enkripsi. Halaman dekripsi dapat dilihat pada Gambar 10.



Gambar 10 Tampilan halaman proses dekripsi

Pada proses dekripsi berikut ini mengambil nilai koordinat f (202,300) pada file citra yang sebelumnya telah dienkripsi dengan nilai R =201, G =259, B =74, dengan menggunakan persamaan (4) dan (5) maka proses dekripsi dilakukan seperti berikut.

$$(ax)^{-1} = a^{317-1-152} \bmod 317$$
$$= 7^{164} \bmod 317$$
$$= 42$$
$$m(R) = b/ax \bmod p$$
$$= 201 * 42 \bmod 317$$
$$= 200$$
$$m(G) = b/ax \bmod p$$
$$= 259 * 42 \bmod 317$$
$$= 100$$
$$m(B) = b/ax \bmod p$$
$$= 74 * 42 \bmod 317$$
$$= 255$$

Setelah proses dekripsi dilakukan dapat disusun kembali titik koordinat f (202,300) menjadi (200 100 255). Berikut ini adalah susunan nilai RGB *plaintext* suatu file setelah dilakukan proses dekripsi.

	1			2			...	300		
	R	G	B	R	G	B	...	R	G	B
1	255	255	255	150	150	0	...	100	0	255
2	200	200	150							
...		...								
202	120	0	220					200	100	255

Gambar 11 Nilai RGB *Plaintext*

Jadi nilai RGB dari citra yang merupakan hasil dari proses dekripsi bernilai sama dengan nilai RGB pada citra sebelum dilakukan proses enkripsi.

IV. SIMPULAN

Simpulan yang diperoleh setelah melakukan perancangan, pembuatan dan pengujian program Sistem Kriptografi ElGamal yaitu:

a. File bitmap dapat diubah ekstensinya menjadi "este" melalui proses enkripsi dan dapat dikembalikan menjadi file berekstensi bitmap lagi melalui proses dekripsi.
b. Aplikasi yang dihasilkan hanya dapat digunakan untuk file tipe bitmap dengan format piksel 24 bit.

DAFTAR PUSTAKA

[1] Achmad, Balza dan Firdausy, Kartika. *Teknik Pengolahan Citra Digital Menggunakan Delphi.* Andi Publishing, Yogyakarta. 2005.

[2] Divisi Litbang Madcoms. *Pemrograman Delphi 7 (Jilid 2).* Andi, Yogyakarta. 2003.

[3] Husni. *Pemrograman Database Dengan Delphi.* Graha Ilmu, Yogyakarta. 2004.

[4] Irawati. *Simulasi Sistem Keamanan Data Menggunakan Metode Public Key Cryptography.*Tugas Akhir, Teknik Elektro Universitas Muhammadiyah Purwokerto. 2007.

[5] Ladjamudin, Al Bahra Bin. *Rekayasa Perangkat Lunak.* Graha Ilmu, Yogyakarta. 2006.

[6] Munir,Rinaldi. *Pengolahan Citra Digital Dengan Pendekatan Algoritmik.* Informatika, Bandung. 2008.

[7] Novia, Dewi. *Aplikasi Teori Bilangan Bulat pada Kriptografi Model RSA dan ElGamal.* Skripsi, Fakultas Keguruan dan Ilmu Pendidikan Universitas Muhammadiyah Purwokerto. 2009.