Penerapan Algoritma Kriptografi Asimetris *Elgamal* dengan Modifikasi Pembangkit Kunci terhadap Enkripsi dan Dekripsi Gambar Warna

Nonik Indahwati[1], Agus Prihanto[2],

[1] Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya

[2]Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya

[1]nonikindahwati@mhs.unesa.ac.id

[2]agusprihanto@unesa.ac.id

***Abstrak*— Perkembangan yang terjadi pada teknologi digital diikuti pula dengan perkembangan perilaku pada masyarakat yang dengan mudahnya menciptakan data maupun mengakses data pada media digital, kemudahan menggunakan media digital untuk mendokumentasikan momen dalam bentuk foto maupun video. Hal tersebut bukan hanya menimbulkan sebuah peluang dalam pengembangan aplikasi, namun juga akan membuka peluang adanya ancaman terhadap manipulasi, perusakan hingga pencurian data tersebut. Pentingnya nilai dari data dan informasi mengakibatkan data hanya boleh diakses oleh orang tertentu, apalagi jika data dan informasi tersebut merupakan aset bernilai yang diharuskan untuk dilindungi dengan perlindungan yang aman. Pada keamanan jaringan sangat diperlukan untuk menanggulangi ancaman pencurian data tersebut sehingga membutuhkan sebuah penerapan mekanisme keamanan jaringan menggunakan teknik-teknik penyandian. Penelitian ini mencoba untuk membuat sistem yang digunakan untuk proses enkripsi dan dekripsi gambar warna yang menggunakan algoritma asimetris *elgamal* dengan modifikasi pada pembangkit kunci. Adapun metode yang digunakan adalah algoritma *elgamal*.**

Pada penelitian ini algoritma *elgamal* dengan modifikasi pembangkit kunci mampu dengan baik memproses enkripsi dan dekripsi pada gambar warna. Perbandingan antara gambar asli dan gambar yang telah dienkripsi menggunakan PSNR (Peak Signal Noise Ratio). Secara keseluruhan sistem yang dihasilkan dari penelitian ini sudah berjalan dengan baik dan sesuai dalam melakukan enkripsi dan dekripsi. Waktu yang dibutuhkan untuk melakukan proses bergantung pada ukuran *file* serta untuk proses enkripsi lebih lama dibandingan dengan waktu yang dibutuhkan untuk proses dekripsi. Hasil perbandingan dari gambar yang diuji coba menghasilkan beberapa perbedaan yaitu gambar asli dengan gambar setelah dienkripsi terdapat perbedaan, sedangkan perbandingan gambar asli dengan gambar setelah didekripsi tidak terdapat perbedaan.

***Kata Kunci*— Algoritma Elgamal, Kriptografi, Enkripsi, Dekripsi, Gambar Warna.**

I. PENDAHULUAN

Kriptografi merupakan sebuah istilah yang berasal dari bahasa Yunani yang mana terdiri dari kata *cryptos* berarti tersembunyi dan *graphein* yang berarti menulis [6]. Bidang ilmu komputer dan matematika yang berfokus pada teknik untuk keamanan komunikasi antara dua pihak sementara terdapat pula pihak ketiga [8]. Maka dengan adanya kriptografi dapat mengamankan data dari serangan atau pencurian data dari orang-orang yang tidak bertanggung jawab. Adapun macam dari kriptografi dibagi menjadi dua yaitu kriptografi klasik yang merupakan suatu algoritma yang mana hanya menggunakan satu kunci untuk mengamankan data, serta kriptografi modern yang mana kriptografi modern ini mempunyai kerumitan yang sangat kompleks karena pada proses enkripsi dan dekripsinya dioperasikan menggunakan komputer.

Gambar atau sketsa dapat didefinisikan sebagai hasil buatan dari benda seperti manusia, hewan, tanaman, dan lain-lain yang dihasilkan dari buatan tangan atau alat penghasil media gambar tersebut. Terdapat beberapa aktifitas manusia khususnya pertukaran data yang menggunakan objek gambar. Gambar atau citra memiliki elemen yaitu piksel yang merupakan komponen gambar terkecil, memiliki nilai numerik intensitas piksel yang berkisar antara hitam dan putih [5]. Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi seiring dengan perkembangan teknologi yang terjadi serta banyaknya pertukaran informasi setiap detiknya di internet. Hal tersebut memicu adanya kejadian pencurian atas informasi oleh pihak -pihak yang tidak bertanggung jawab. Terdapat empat ancaman keamanan yang terjadi terhadap data atau informasi seperti kerahasiaan, keutuhan data, dan auntetikasi entitas [9]. *Interruption* yang merupakan ancaman terhadap *availability* informasi yaitu data yang ada dalam sistem komputer dirusak atau dihapus sehingga jika data atau informasi tersebut dibutuhkan maka pemiliknya akan mengalami kesulitan untuk mengaksesnya atau mungkin hilang, *interception* merupakan ancaman terhadap kerahasiaan (*secrecy*) yaitu informasi disadap sehingga orang yang tidak berhak dapat mengakses komputer dimana data disimpan, *modification* yang merupakan ancaman terhadap integritas data yaitu penyadapan terhadap informasi lalu lintas informasi yang sedang dikirim kemudian diubah sesuai dengan keinginan penyadap, dan *fabrication* berupa ancaman terhadap integritas yang mana merupakan orang yang tidak berhak berhasil melakukan peniruan atau pemalsuan informasi sehingga terjadi kesalahfahaman bahwa informasi tersebut berasal dari orang yang dikehendaki [2].

Proses enkripsi dan dekripsi dengan algoritma elgamal lebih menggunakan perhitungan algortima matematika yang rumit [7]. Berdasarkan hal tersebutlah dilakukan penelitian menggunakan algoritma asimetris elgamal dengan memodifikasi pembangkit kunci. Algoritma elgamal merupakan algoritma blok *cipher* yaitu algoritma yang mana proses enkripsi dilakukan pada blok-blok *plain text* yang kemudian akan menghasilkan blok-blok *cipher text* lalu akan didekripsi kembali dan hasilnya akan digabungkan menjadi *plain text* semula [5]. Pada proses pembangkitan kuncinya menggunakan logaritma diskrit dan metode enkripsi dekripsi yang menggunakan proses komputasi yang besar sehingga menghasilkan enkripsi dengan ukuran dua kali lipat dari ukuran semula.

Karena data spesifiknya data gambar rawan terdapat masalah keamanan yang merupakan salah satu aspek terpenting dari sebuah sistem informasi seiring dengan perkembangan teknologi yang terjadi serta banyaknya pertukaran informasi setiap detiknya di internet. Hal tersebut memicu adanya kejadian pencurian atas informasi oleh pihak -pihak yang tidak bertanggung jawab. Adapun hal yang bersifat pribadi dan rahasia maka hal tersebut menjadi suatu yang penting untuk diperhatikan keamanannya, maka salah satu upaya untuk mengamankan data yang berupa gambar warna adalah dengan melakukan penerapan suatu modifikasi algoritma kriptografi *elgamal* terhadap enkripsi dan dekripsi gambar.

II. PENELITIAN TERKAIT

Binantara Permadi telah melakukan penelitian dengan judul Implementasi Algoritma Kriptografi *Elgamal* pada Data Text. Algoritma kriptografi *elgamal* diimplentasikan pada aplikasi *client* untuk mengenkripsi suatu data teks dan dihasilkan sebuah program aplikasi enkripsi dan dekripsi *elgamal* yang dibangun menggunakan delphi yang dapat digunakan oleh *user* secara umum. Program aplikasi yang dihasilkan merupakan aplikasi yang dapat mengubah *file* atau teks asli menjadi *file* yang terenkripsi dimana isi *file* tidak dapat dibaca serta dapat mengembalikan *file* atau teks yang tidak bisa dibaca menjadi *file* aslinya dengan metode *elgamal* tanpa merusak dan merubah isi *file* tersebut. Terdapat batasan *file* dimana hanya menggunakan *file* berbentuk txt serta kasus pengenalan /n sebagai spasi juga belum ada [1].

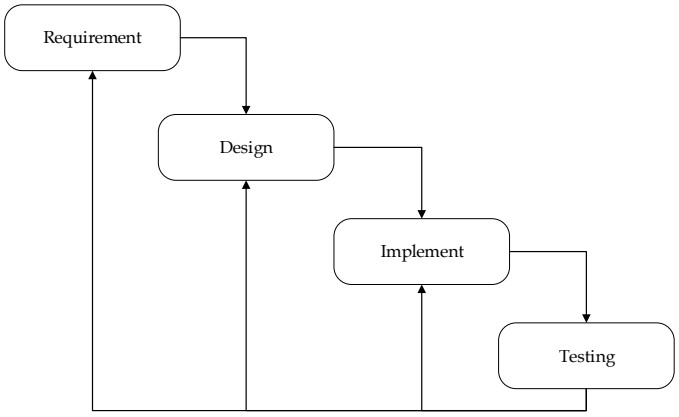
Terdapat sebuah penelitian yang melakukannya menggunakan syarat bilangan prima yang dimulai dari lima atau lebih dari lima, menggunakan SSL sebagai protokol yang mengamankan komunikasi antara *client* dan *server*, serta menggunakan implementasi aplikasi *group chat*. Terdapat sebuah langkah yang mana memasukkan data berupa teks ke basis data lalu memunculkan kembali data tersebut dari basis data ke antarmuka sistem dan menghasilkan konklusi yaitu masukan awal yang persis tidak mendapatkan kecepatan yang persis sebab hasil *cipher text* juga berbeda serta karakter yang sedikit juga bukan berarti akan menghasilkan waktu yang cepat. Pengujian aplikasi menggunakan teknik *sniffing* dibuat jaringan lokal yang ingin menyadap data dengan menggunakan alat penyadapan yang tersedia. Dengan menggunakan aturan *secure socket layer* maka hal tersebut dapat membentengi *user* dari kejahatan penyadapan data. Pada aplikasi yang dihasilkan belum ada pilihan masukan berupa dokumen, foto dan emoji, layanan *group chat* belum bisa berjalan secara *online* dan tidak ada layanan obrolan pribadi yang menyebabkan pengguna belum bisa membuat hubungan atau koneksi antar anggota [2].

Hasil penelitian yang dilakukan oleh Faqihuddin Al-Anshori dan Eko Aribowo menyatakan bahwa data file yang dapat dienkripsi dalam sistem ini adalah data file yang berbentuk rtf, txt dan pesan singkat, menghasilkan sebuah program aplikasi yang dapat mengubah file asli menjadi file yang terenkripsi dimana isi file tidak dapat dibaca, dapat mengembalikan file yang tidak bisa dibaca menjadi file aslinya dengan metode elgamal tanpa merusak dan mengubah isi file tersebut, serta dapat mengubah pesan asli berupa *plain text* menjadi *cipher text* yaitu berupa kode-kode yang tidak bisa terbaca [3].

Penelitian enkripsi dan dekripsi gambar dilakukan oleh Hayder Raheem Hashim dan Irtifaa Abdalkadum Neamaa [4]. Dengan menambahkan modifikasi *cryptosystem* yaitu diterapkan pada gambar abu-abu dan warna dengan mengubah gambar menjadi matriks yang sesuai menggunakan program *matlab*, kemudian menerapkan algoritma enkripsi dan dekripsi di atasnya untuk memberikan *cryptosystem* yang lebih aman dan kebal terhadap beberapa serangan dari sebelumnya. Baik gambar warna dan *grayscale* dengan berbagai ukuran disimpan dalam *Portable Network Graphics* (PNG) dan hasilnya menunjukkan gambar asli (warna dan skala abu-abu) dan gambar terenkripsi.

III. METODOLOGI PENELITIAN

Berikut ini merupakan alur jalannya diagram penelitian untuk melakukan proses "Penerapan Algoritma Kriptografi Asimetris *Elgamal* dengan Modifikasi Pembangkit Kunci terhadap Enkripsi dan Dekripsi Gambar Warna" :

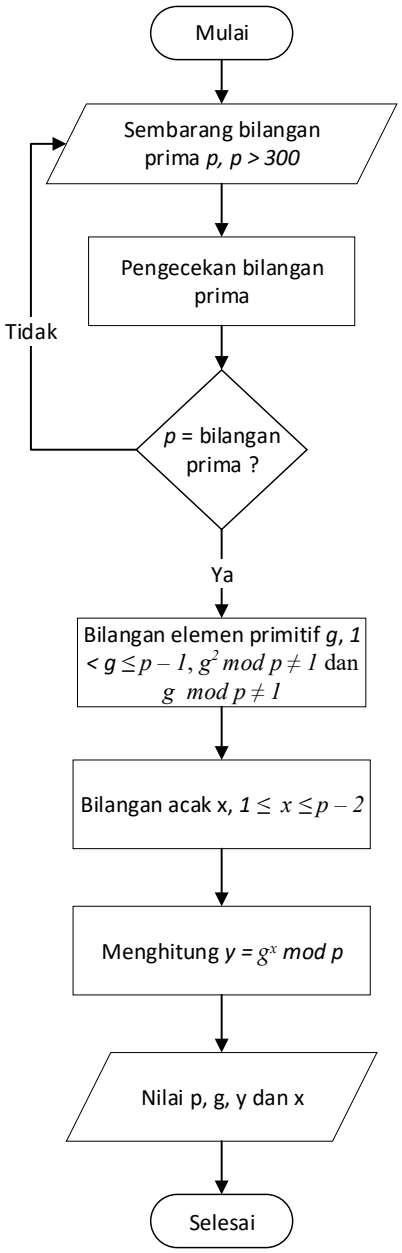


Gbr. 1 Metode Penelitian

Penelitian mengenai proses enkripsi dan dekripsi gambar warna menggunakan algoritma asimetris elgamal dengan memodifikasi pembentukan kunci. Dengan menggunakan algoritma elgamal yang dimodifikasi pembangkit kuncinya, maka proses enkripsi dan dekripsi akan dianalisis hasil kunci, efisiensinya yang meliputi kecepatan waktu proses, perubahan ukuran gambar, serta perbedaan gambar. Adapun tahapan yang dilakukan pada penelitian ini adalah sebagai berikut :

A. Proses Pembentukan Kunci

Pada tahap pembentukan kunci ini merupakan sebuah proses dimana proses ini digunakan untuk membangkitkan kunci yang digunakan untuk proses enkripsi dan dekripsi. Pada algoritma *elgamal* terdapat pembentukan kunci yaitu ditunjukkan pada Gbr. 2 berikut ini :



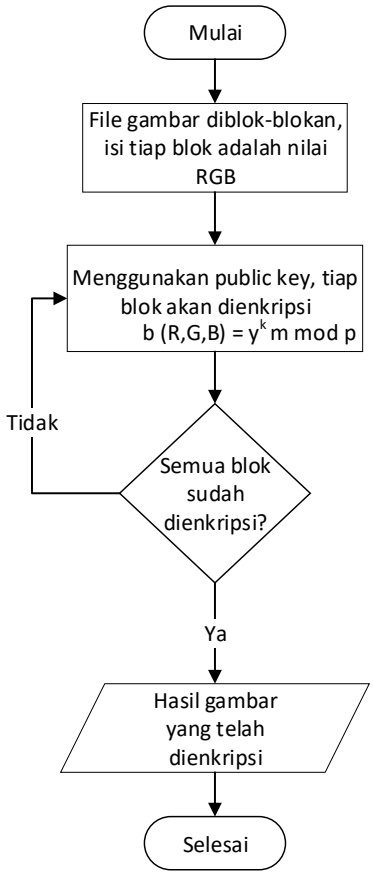
Gbr. 2 Alur Pembangkitan Kunci

Berikut merupakan langkah-langkah dalam pembuatan kunci :

1. Sembarang bilangan prima p, dengan syarat p > 300.
2. Pilih bilangan acak g dengan syarat g < p.
3. Pilih bilangan acak x dengan syarat 1 ≤ x ≤ p – 2.
4. Hitung y = g^x mod p.
5. Hitung a = g^k mod p.
6. Hitung ax = a^{p-1-x} mod p.

B. Proses Enkripsi

Pada tahap proses enkripsi ini merupakan proses untuk mengubah data gambar menjadi *file cipher image* dengan menggunakan nilai-nilai kunci publik.

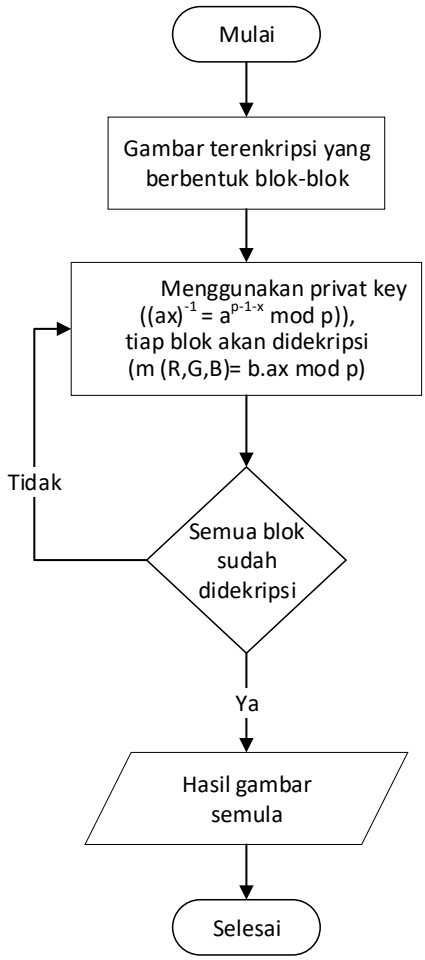


Gbr. 3 Alur Proses Enkripsi Algoritma Elgamal

1. Langkah pertama sebelum melakukan proses enkripsi yaitu memasukkan kunci publik atau *public key*.
2. Lalu mengambil gambar *plain image*.
3. Dengan menggunakan kunci publik atau *public key*, setiap blok (piksel) akan dienkripsi.
4. Menggunakan rumus b (R, G, B) = y^k m mod p
5. Pengecekan agar semua blok terenkripsi.
6. Hasil *cipher image*.

C. Proses Dekripsi

Pada tahap proses dekripsi ini merupakan proses yang digunakan untuk mengubah gambar yang telah dienkripsi menjadi gambar awal.



Gbr. 4 Alur Proses Dekripsi Algoritma Elgamal

Proses dekripsi merupakan proses dimana pengembalian *cipher image* menjadi *plain image* atau data seperti semula. Pada proses ini membutuhkan kunci privat yang mana hanya boleh diketahui oleh orang yang dikehendaki saja. Penjelasannya adalah sebagai berikut :

1. Langkah awal yaitu mencari atau memasukkan gambar yang akan didekripsi atau *cipherimage*.
2. Kemudian mengambil atau memasukkan kunci pribadi.
3. Menggunakan kunci pribadi atau *private key*, lalu setiap blok (piksel) akan didekripsi.
4. Dengan rumus m (R, G, B) = b.ax mod p
5. Pengecekan agar semua blok terdekripsi.
6. Lalu akan menghasilkan gambar sesuai dengan data sebelum dienkripsi.

IV. HASIL DAN PEMBAHASAN

A. *Data Penelitian*

Tahap pertama dalam melakukan penelitian ini adalah penentuan dan kesiapan data yaitu gambar yang akan menjadi uji coba dalam proses enkripsi dan dekripsi. Data gambar yang digunakan dalam penelitian ini diberikan identitas atau kode gambar. Pada tabel III berikut merupakan kumpulan data yang diuji coba :

TABEL I
DATA GAMBAR PENELITIAN

No.	Gambar	Kode File	Dimensi File	Ukuran File
1.		A1	455x303	238 KB
2.		A2	779x584	762 KB
3.		A3	998x561	1,31 MB
4.		A4	1920x1280	4,00 MB
5.		A5	3840x2400	5,90 MB
6.		A6	3872x2592	15,9 MB

B. *Hasil Pengujian*

Dalam hal ini telah dilakukan pengujian enkripsi dan dekripsi terhadap sistem yang telah dibuat, pengujian terhadap penelitian ini dilakukan menggunakan sampel data yang diambil dari sumber yang telah ditentukan sebelumnya. Hasil pengujian ukuran *file* algoritma elgamal sebelum dan sesudah dimodifikasi sebagai berikut :

TABEL II
PERBANDINGAN UKURAN GAMBAR

		Sebelum Modifikasi		Setelah Modifikasi	
No.	Kode File	Plain Image	Cipher Image	Plain Image	Cipher Image
1.	A1	238 KB	374 KB	238 KB	420 KB
2.	A2	762 KB	1,34 MB	762 KB	1,32 MB
3.	A3	1,31 MB	2,14 MB	1,31 MB	2,09 MB
4.	A4	4,00 MB	6,49 MB	4,00 MB	7,35 MB
5.	A5	5,90 MB	14,5 MB	5,90 MB	13,8 MB

No.	Kode File	Sebelum Modifikasi		Setelah Modifikasi	
		Plain Image	Cipher Image	Plain Image	Cipher Image
6.	A6	15,9 MB	29,6 MB	15,9 MB	30,6 MB

Hasil analisis dan pengujian yang diperoleh dapat terlihat berdasarkan perbandingan gambar sebelum proses enkripsi dan setelah dienkripsi menggunakan algoritma elgamal. Sedangkan berdasarkan hasil yang dilakukan pada pembentukan kunci yang digunakan untuk proses enkripsi dan dekripsi menghasilkan kunci yang dituliskan pada tabel III dan tabel IV berikut ini :

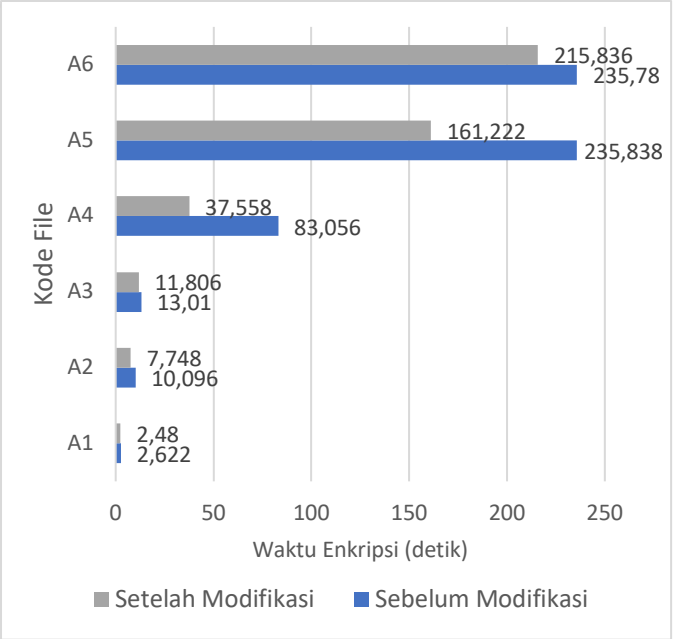
TABEL III
HASIL ANALISIS KUNCI SEBELUM DIMODIFIKASI

No.	Kode File	Kunci Enkripsi	Kunci Dekripsi
1.	A1	y: 135, k: 104, p: 263	g: 85, k: 104, p: 263, x: 257
2.	A2	y: 243, k: 316, p: 479	g: 141, k 316, p: 479, x:362
3.	A3	y 149, k: 291, p: 383	g: 191, k:291, p:383, x:178
4.	A4	y: 351, k: 435, p: 467	g: 454, k: 435, p: 467, x:46
5.	A5	y: 274, k: 427, p: 347	g: 72, k: 427, p: 347, x: 261
6.	A6	y: 385, k: 396, p: 467	g: 59, k: 396, p: 467, x: 70

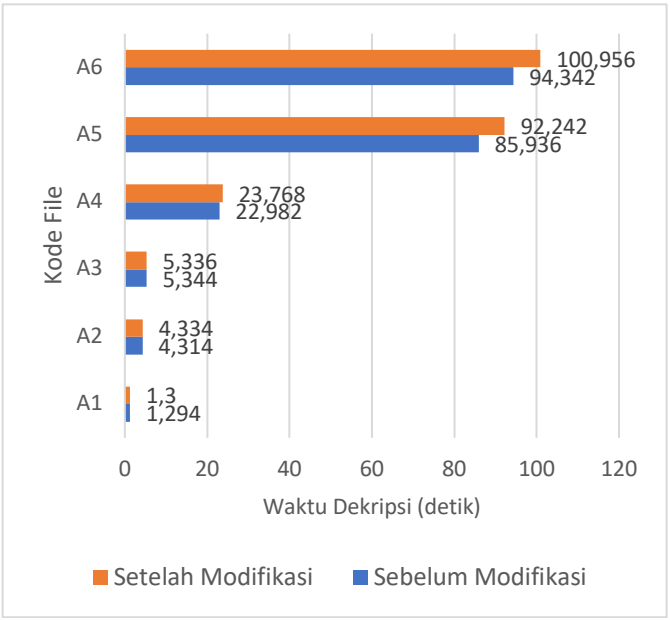
TABEL IV
HASIL ANALISIS KUNCI SETELAH DIMODIFIKASI

No.	Kode File	Kunci Enkripsi	Kunci Dekripsi
1.	A1	y: 299, k: 37, p: 467	g: 288, k: 37, p: 467, x:228
2.	A2	y: 261, k: 159, p: 383	g:182, k: 159, p:383, x:204
3.	A3	y: 140, k: 266, p: 383	g:221, k: 266, p:383, x:355
4.	A4	y: 157, k: 47, p: 467	g: 63, k: 47, p: 467, x: 430
5.	A5	y: 45, k: 383, p: 467	g:118, k:383, p: 467, x:287
6.	A6	y: 246, k: 470, p: 347	g:136, k: 470, p:347, x:209

Berdasarkan hasil uji coba yang telah dilakukan pada proses enkripsi dan dekripsi pada gambar warna dihasilkan waktu yang digunakan dalam proses yang dilakukan sebanyak lima kali. Maka dihasilkan perbandingan waktu (satuan detik) enkripsi dan dekripsi yang dituliskan dalam diagram sebagai berikut :

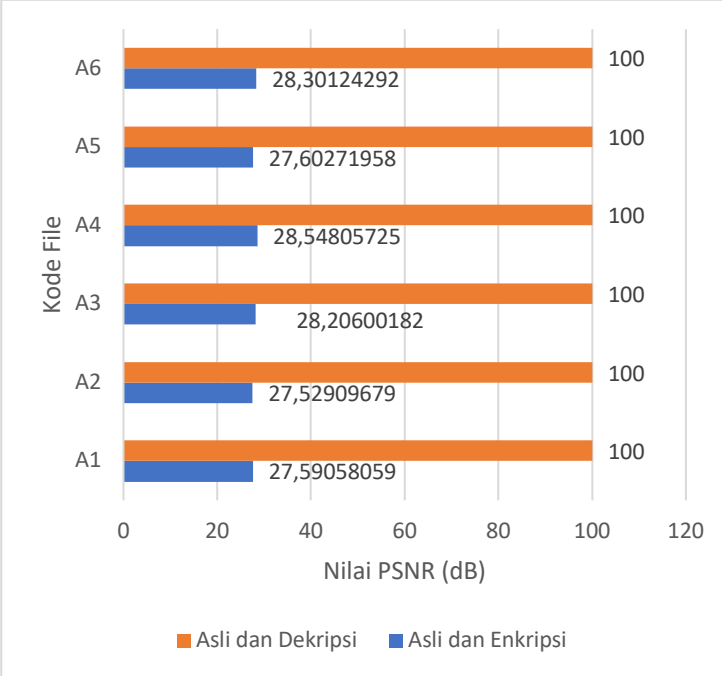


Gbr 5. Perbandingan Waktu Enkripsi



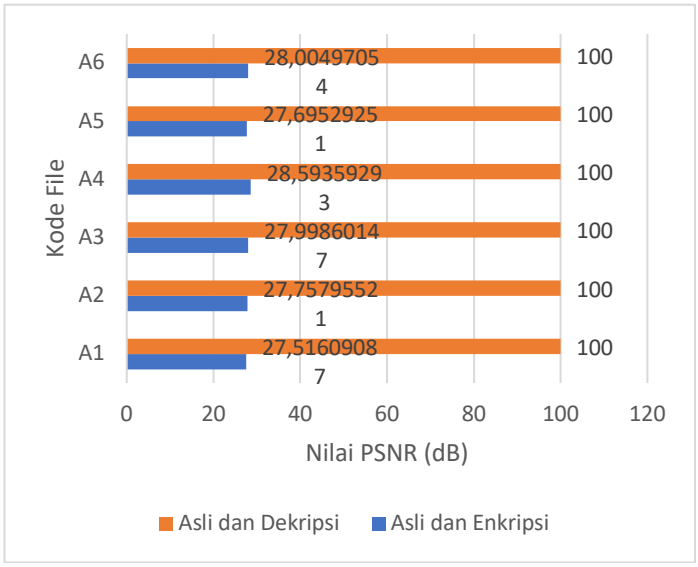
Gbr. 6 Perbandingan Waktu Dekripsi

Kemudian berdasarkan pengujian yang telah dilakukan terhadap gambar dengan menggunakan pengujian pada perbandingan kemiripan antara gambar asli dan gambar yang telah dienkripsi serta gambar yang asli dan gambar setelah didekripsi menggunakan PSNR (Peak Signal Noise Ratio) yang sering dinyatakan dalam skala logaritmik dalam decibel (dB) dihasilkan grafik perbandingan tersebut. Apabila nilai PSNR jatuh dibawah 30 dB maka itu berarti perbandingan terlihat jelas. Akan tetapi jika kualitas dan tingkat kemiripan gambar yang tinggi maka PSNR berada pada nilai 40dB dan diatasnya karena sedikit atau tidak ada perbedaan pada gambar. Hasil dari analisis yang dilakukan maka dihasilkan perbandingan yang dituliskan dalam tabel sebagai berikut :



Gbr. 7 Perbandingan Gambar Sebelum Modifikasi dengan PSNR

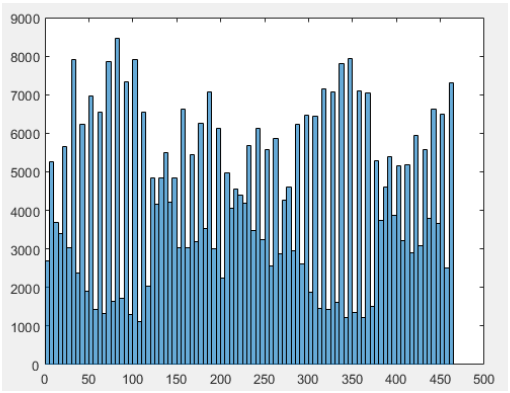
Dari diagram pada gambar 7 dapat diketahui bahwa uji coba sebelum dimodifikasi perbandingan kemiripan gambar asli dan gambar yang telah dienkripsi terdapat perbedaan yaitu kemiripan dengan nilai 27-28 akan tetapi perbandingan gambar asli dan dekripsi tidak memiliki perbedaan atau mempunyai kemiripan 100.



Gbr. 8 Perbandingan Gambar Setelah Modifikasi dengan PSNR

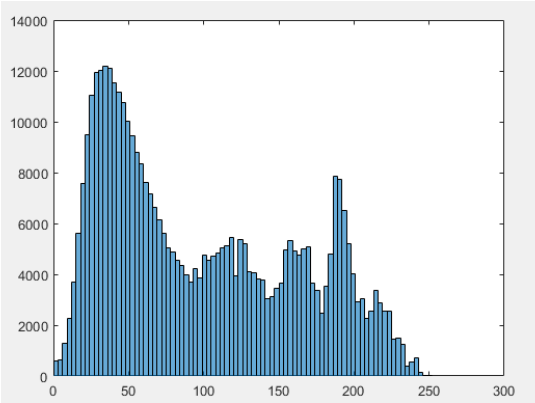
Berdasarkan diagram pada gambar 8 dapat diketahui bahwa uji coba setelah dimodifikasi perbandingan gambar asli dan gambar yang telah dienkripsi terdapat perbedaan yaitu memiliki kemiripan dengan nilai 27-28 akan tetapi perbandingan gambar asli dan dekripsi tidak memiliki perbedaan atau mempunyai kemiripan 100.

Adapun pengujian perbandingan kemiripan antara gambar asli dan gambar yang telah dienkripsi dengan proses enkripsi dan dekripsi sebelum dimodifikasi dan sesudah dimodifikasi yang dilakukan dengan menggunakan histogram dengan melihat kemunculan atau intensitas RGB (Red, Green, Blue). Dalam pengujian ini menghasilkan perbandingan yang ditunjukkan pada diagram berikut :



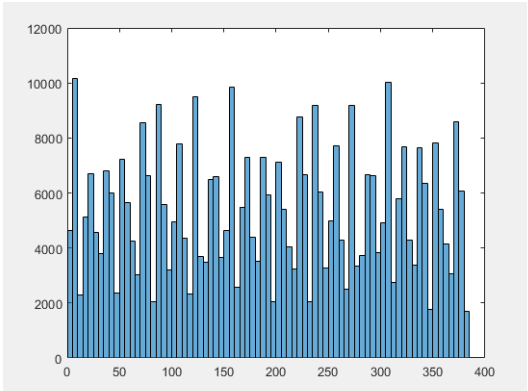
Gbr. 9 Histogram Cipher Image Sebelum Modifikasi

Penyebaran nilai-nilai intensitas piksel dari *cipher image* dengan algoritma sebelum dimodifikasi yang telah diuji yaitu distribusi nilai intensitas *cipher image* memiliki nilai piksel dalam rentang 0 sampai dengan kurang dari 500.



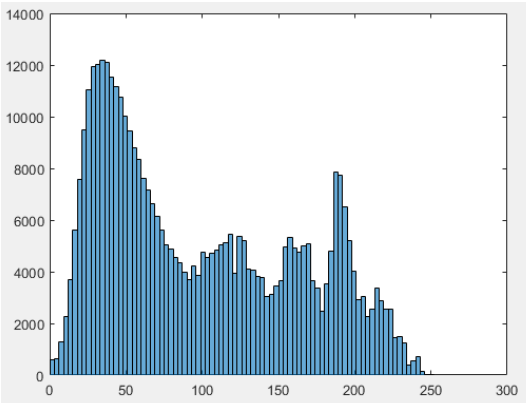
Gbr. 10 Histogram Plain Image Sebelum Modifikasi

Penyebaran nilai-nilai intensitas piksel dari *plain image* dengan algoritma sebelum dimodifikasi yang telah diuji yaitu histogram gambar berada pada rentang nilai intensitas 0-255.



Gbr. 11 Histogram Cipher Image Setelah Modifikasi

Penyebaran nilai-nilai intensitas piksel dari *cipher image* dengan algoritma setelah dimodifikasi yang telah diuji yaitu memiliki nilai piksel dalam rentang 0 sampai dengan kurang dari 400.



Gbr. 12 Histogram Plain Image Setelah Modifikasi

Penyebaran nilai-nilai intensitas piksel dari *plain image* dengan algoritma setelah dimodifikasi yang telah diuji yaitu histogram gambar yang berada pada rentang nilai intensitas 0-255 dengan intensitas kemunculan yang berbeda-beda.

V. KESIMPULAN

Kesimpulan yang diperoleh dari seluruh proses dan hasil pembahasan penelitian yang telah dilakukan yaitu dapat menghasilkan sebuah sistem yang dapat melakukan enkripsi dan dekripsi menggunakan algoritma asimetris elgamal yang memiliki tampilan antarmuka. Dalam uji coba yang telah dilakukan, pada analisis proses enkripsi dan dekripsi yang telah dilakukan uji coba berjalan dengan baik. Modifikasi pada pembangkit kunci yang dilakukan menghasilkan kecocokan kunci yang baik. Perbandingan kemiripan yang terdapat pada gambar asli dengan gambar setelah dienkripsi terdapat perbedaan, sedangkan perbandingan kemiripan gambar asli dengan gambar setelah didekripsi tidak terdapat perbedaan. Waktu dibutuhkan pada proses enkripsi lebih lama dibandingan waktu yang dibutuhkan pada proses dekripsi, serta untuk proses enkripsi dan dekripsi pada gambar dengan ukuran besar membutuhkan waktu lebih lama dibandingkan pada gambar ukuran kecil, sehingga lama waktu yang dihasilkan dalam melakukan proses enkripsi dan dekripsi dipengaruhi juga oleh ukuran gambar.

UCAPAN TERIMA KASIH

Puji syukur serta rasa terima kasih saya haturkan kepada Allah SWT yang selalu memberi kemudahan dan kelancaran dalam mengerjakan jurnal ini. Semua pihak terkait yang senantiasa memberi saran serta semangat sehingga jurnal ini dapat terselesaikan dengan baik.

REFERENSI

[1] B. Parmadi, "Implementasi Algoritma Kriptografi Elgamal pada Data Text," pp. 1-5, 2017.

[2] H. Aditya, I. N. Farida and R. A. Ramadhani, "Penerapan Algoritma Elgamal dan SSL pada Aplikasi Group Chat," *Generation Journal,* pp. 48-56, 2018.

[3] F. Al-Anshori and E. Aribowo, "Implementasi Algoritma Kriptografi Kunci Publik Elgamal untuk Proses Enkripsi dan Dekripsi guna Pengamanan File Data," *Jurnal Sarjana Teknik Informatika,* pp. 376-384, 2014.

[4] H. R. Hashim and I. A. Neamaa, "Image Encryption and Decryption in A Modification of ElGamal Cryptosystem in MATLAB," *International Journal of Sciences : Basic and Applied Research (IJSBAR) ,* pp. 141-147, 2014.

[5] R. A. Asmara, Pengolahan Citra Digital, 1st ed., Malang: POLINEMA PRESS, 2018.

[6] D. Ariyus, Kriptografi, Yogyakarta: Graha Ilmu, 2006.

[7] D. Ariyus, PENGANTAR ILMU KRIPTOGRAFI Teori Analisis dan Implementasi, Yogyakarta: C.V ANDI OFFSET (Penerbit ANDI), 2008.

[8] M. Barakat, C. Eder and T. Hanke, An Introduction to Cryptography, Kaiserslautern: TU Kaiserslautern, 2018.

[9] R. Sadikin, Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java, Yogyakarta: Penerbit Andi, 2012.