PROSIDING

Seminar Nasional Teknologi, Kualitas dan Aplikasi

SEMINAR NASIONAL TEKNOKA 4

Seminar Nasional Teknologi, Kualitas dan Aplikasi 2019

INOVASI TEKNOLOGI: *SMART, LEAN AND GREEN* DI ERA DISRUPTIF

Sabtu, 30 November 2019

08.00 - 16.30 WIB

Aula Ahmad Dahlan Lantai 6
Gedung A FKIP UHAMKA
Jl. Tanah Merdeka Kp. Rambutan,
Ciracas, Jakarta Timur

PEMBICARA

Dr. Ir. Bambang Setiadi, IPU
Ketua Dewan Riset Nasional

Prof. Dr. Ing. Mudrik Alaydrus
Professor in Electrical Engineering

Muhammad Salis
Product Engineer Go-Jek

PENYELENGGARA : FAKULTAS TEKNIK UHAMKA
Jl. Tanah Merdeka No. 6 Kp. Rambutan, Ciracas, Jakarta Timur
(021) 8400941 (021) 87782739
teknoka@uhamka.ac.id teknoka.uhamka.ac.id

PROSIDING
Seminar Nasional TEKNOKA
(Teknologi, Kualitas dan Aplikasi) ke – 4

“INOVASI TEKNOLOGI: SMART, LEAN AND GREEN DI ERA DISRUPTIF”

Teknoka@2019

PROSIDING
Seminar Nasional TEKNOKA
(Teknologi, Kualitas dan Aplikasi) ke – 4
ISSN Cetak 2502-8782 / ISSN Online 2580-6408

Reviewer (Penelaah)

1. Prof. Dr. Makbul Anwari (Department of Electrical Engineering and Computer Engineering, Faculty of Engineering, King Abdulaziz University, Saudi Arabia).
2. Prof. Ir. Erry Yulian Triblas Adesta, M.Sc, IPM (Department of Mechanical Engineering, Faculty of Engineering, International Islamic University of Malaysia, Kuala Lumpur, Malaysia).
3. Dr. Ir. Yohannes Dewanto (Program Studi Teknik Elektro, Fakultas Teknik, Universitas Suryadarma, Jakarta, Indonesia).
4. Roer Eka Pawinanto, M.Sc, PhD (Malaysia Japan International Institute of Technology, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia).
5. Ir. Harry Ramza, MT, PhD (Program Studi Teknik Elektro, FT – UHAMKA, Jakarta, Indonesia).
6. Dr. Dan Mugisidi, M.Si (Program Studi Teknik Mesin, FT – UHAMKA, Jakarta).
7. Arafat Febriandirza, MTI, PhD (Program Studi Teknik Informatika, FT – UHAMKA, Jakarta, Indonesia).
8. Atiqah Meutia Hilda, S.Kom, M.Kom (Program Studi Teknik Informatika, FT – UHAMKA, Jakarta, Indonesia).
9. Wildan Thoyib, ST, M.Eng (Program Studi Teknik Informatika, FT – UHAMKA, Jakarta, Indonesia).
10. Dwi Astuti Cahyasiwi, ST, MT (Program Studi Teknik Elektro, FT – UHAMKA, Jakarta, Indonesia).

Ketua Editor
Ir. Harry Ramza, MT, PhD

Editor Anggota
Emilia Roza, ST., M.Pd., MT
Arien Bianingrum, S. Sos
Nunik Pratiwi, ST, M.Kom
Lutfan Zulwaqor, S.IP
M. Mujirudin,ST., MT.

Administrasi
Sadiro, S.Pd
Herman Fauzi

Alamat
Fakultas Teknik, Universitas Muhammadiyah Prof. Dr. HAMKA
Jalan Tanah Merdeka No. 6, Kp Rambutan, Jakarta 13540
Telp : +62 – 21 – 8400941 / Faks : +62 – 21 – 8778 2739

DAFTAR ISI

TEKNIK INFORMATIKA

SEMINAR NASIONAL TEKNOKA

Vol. 4, 2019
ISSN No. 2502-8782

Implementasi Algoritma ElGamal Dalam Proses Enkripsi dan Dekripsi Untuk Pengamanan Citra Digital Pada Perangkat Mobile

Fachriyan Rizki Ibrahim[1], Arry Avorizano, M.Kom[2]

[1,2)]Fakultas Teknik UHAMKA,
Jl. Tanah Merdeka No.6, RT.10/RW.3, Jakarta Timur, Telp: 8400941, Mobile: 085813001800
E-mail: fachriyanri@gmail.com [1]arry.avorizano@uhamka.ac.id [2]

Abstrak – *Implementasi keamanan data adalah salah satu cara efektif dalam mengamankan data demi melindungi privasi dan keaslian data milik pengguna. Subjek dalam penelitian adalah bagaimana cara melindungi suatu file citra digital. Metode yang digunakan adalah Kriptografi ElGamal, metode tersebut adalah suatu bagiana dari kriptografi asimetris. Terdapat tiga proses didalam Kriptogtafi ElGamal, yaitu proses pembuatan kunci, proses enkripsi data dan proses dekripsi data. Metode yang digunakan pada penelitian ini adalah research dan development (R&D) yang dimulai dari identifikasi masalah sampai produksi prototipe akhir.*
Hasil dari penelitian ini di implementasikan dalam suatu program perangkat lunak pada perangkat Android dengan menggunakan bahasa pemrograman Java yang dapat memberikan kemudahan bagi setiap orang yang ingin mengamankan data – data gambar penting.

***Kata kunci**: ElGamal, Keamanan, Citra Digital, Android, Java.*

1 PENDAHULUAN

Di era digital saat ini banyaknya ponsel dengan spesifikasi kamera yang mumpuni memudahkan pengguna untuk menyimpan gambar langsung di ponsel, tetapi dengan kemudahan penyimpanan tersebut menimbulkan celah keamanan data gambar oleh orang-orang yang tidak bertanggung jawab melakukan pencurian data gambar pribadi, memanipulasi gambar, dan mengubah isi gambar tanpa izin dari pemilik gambar yang bersangkutan.

Berbagai macam cara menyembunyikan gambar sudah banyak ditemukan salah satu yang paling banyak digunakan adalah dengan cara melakukan *hidden*, yaitu sebuah teknik penyembunyian *file* agar tidak dapat terbaca dan terlihat. Perkembangan penyembunyian gambar itu sendiri semakin hari semakin pesat. Dengan kata lain gambar yang disembunyikan tersebut sudah tentu banyak orang yang sudah mengetahui cara untuk membukanya, hal ini membuat beberapa instansi yang memiliki gambar yang bersifat penting dan rahasia merasa bahwa ini sudah tidak aman. Karena dengan hanya melakukan *hidden* data citra digital asli dapat langsung terbaca dengan melakukan pengaturan *show hidden file*. Maka dari itu dibutuhkan keamanan tambahan yaitu dengan cara melakukan pengenkripsian data.

Beberapa gambar yang bersifat penting seperti gambar rancangan suatu proyek pembangunan, gambar rangkaian prototipe suatu produk, dan gambar yang bernilai dan bersifat penting lainnya tentu harus dijaga kerahasiaanya agar tidak disalahgunakan oleh pihak luar yang tidak berkepentingan.

Salah satu metode yang dipilih pada penelitian ini adalah metode *ElGamal*. Dengan metode Algoritma *ElGamal* ini keamanan data gambar dapat lebih terjaga kerahasiaannya. Karena algoritma ini memiliki kelebihan antara lain terletak pada metode pembentukan kunci yang menggabungkan antara enkripsi kunci publik dan enkripsi kunci privat sehingga tanda tangan digital atau kunci rahasia tersebut tidak dapat di *kriptanalis*.

Berdasarkan uraian diatas penulis bermaksud mendesain dan merancang suatu aplikasi pada perangkat *mobile* yang berfungsi untuk mengamankan data gambar sehingga keamanan dan privasi dari pemilik gambar akan lebih terjaga.

2 LANDASAN TEORI

Menurut Richard Mollin (2003), Kriptografi (*cryptography*) berasal dari bahasa Yunani terdiri dari dua silabel yaitu *kriptos* dan *graphia*. *Kriptos* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Sedangkan Menurut Menezes, Oorscoot dan Vanstone (1996), kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang

Dipresentasikan pada Tanggal 30 November 2019
DOI: 10.22236/teknoka.v%vi%i.4210

berkaitan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, dan autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu untuk melindungi keamanan sandi.[1]

Bersumber pada sejumlah pengertian kriptografi di atas, dapat disimpulkan bahwa Kriptografi merupakan ilmu sekaligus seni untuk melindungi keamanan pesan dan informasi agar tidak berhasil dilihat, dibaca, dimengerti oleh pihak ketiga yang tidak memiliki wewenang dan otoritas terhadap data atau informasi tersebut.[1]

Kriptanalisis (*cryptanalysis*) adalah kebalikan dari kriptografi, yaitu suatu ilmu untuk memecahkan mekanisme kriptografi dengan cara mendapatkan kunci dari *ciphertext* yang digunakan untuk mendapatkan *plaintext*. Kriptologi *(cryptology)* adalah ilmu yang menggabungkan antara kriptografi dan kriptanalisis.[1]

Algoritma Kriptografi bersumber pada jenis penyandian yang diterapkan dapat dibedakan menjadi dua jenis yaitu :

1. *Symmetric Cryptography* (Kriptografi Simetri), adalah suatu keadaan saat kunci yang digunakan untuk melakukan teknik enkripsi dan teknik dekripsi adalah kunci yang serupa.
2. *Asymmetric Cryptography* (Kriptografi Asimetri), adalah suatu keadaan saat kunci yang digunakan untuk melakukan teknik enkripsi dan teknik dekripsi menggunakan kunci yang berlainan.[5]

Berdasarkan paparan tersebut dapat disimpulkan bahwa kriptografi asimetri mempunyai tingkat proteksi yang lebih baik dibandingkan kriptografi simetri. Pengirim informasi memakai kunci publik untuk melindungi informasi yang ingin disampaikan, kunci publik dapat diketahui oleh seluruh pihak, tetapi kunci publik tidak dapat digunakan untuk membuka informasi dan pesan. Dekripsi informasi hanya dapat dilakukan dengan memakai kunci privat yang hanya bisa diketahui oleh penerima informasi yang sesungguhnya.[5]

Tetapi, Kriptografi Asimetri mempunyai suatu kelemahan yaitu kecepatan yang dimiliki kriptografi asimetri lebih rendah jika dibandingkan kriptografi simetri. Kriptografi Asimetri tidak cocok digunakan untuk melindungi informasi dalam jumlah besar. Dalam implementasinya, pertukaran data di internet, pengiriman *email*, atau transaksi perbankan secara *online* menggunakan metode *hybrid*. Metode *hybrid* melindungi data asli secara simetris, namun kunci yang digunakan secara asimetris. Metode hybrid ini menggabungkan perpindahan kunci yang aman dan enkripsi yang cepat.[5]

Kriptografi tersusun atas dua proses utama yaitu proses enkripsi dan dekripsi.[1]

Enkripsi adalah suatu teknik untuk melakukan pergantian suatu kode dari yang biasa dipahami menjadi suatu kode yang tidak dipahami atau sulit dibaca. Dari definisi di atas dapat disimpulkan Enkripsi adalah mengacak suatu kode menjadi kode lain sehingga tidak dapat diketahui kode aslinya.[2]

Enkripsi pada komputer dilakukan dengan menggeser bit pada karakter ASCII sebanyak x buah ke kiri atau ke kanan, sehingga kata akan teracak dan tidak dapat dibaca, dalam kriptografi enkripsi merupakan suatu hal yang sangat penting agar keamanan data benar – benar terjaga dan bisa dilindungi dengan baik. Pesan asli diubah menjadi suatu kode yang sulit dipahami, enkripsi sendiri bisa diartikan suatu *cipher* atau kode. Agar dapat mengubah ke bentuk awal dari pesan dibutuhkan suatu algoritma yang dapat digunakan untuk mengubah pesan yang diinginkan.[2]

2.1 Hill Cipher

Teknik kriptografi ini dibuat agar dapat menciptakan suatu *cipher* (kode) yang sulit untuk dipecahkan dengan menggunakan metode analisa frekuensi. Teknik ini tidak mengubah masing-masing huruf yang serupa pada *plaintext* dengan huruf lainnya yang serupa pada *chipertext* karena memakai perkalian matriks pada pembentukan enkripsi dan dekripsinya. Teknik kriptografi ini ditemukan pertama kali oleh Lester S.Hill pada tahun 1929.[10]

Berdasarkan jenis penyandian yang diterapkan, kriptografi *Hill Cipher* tergolong kedalam Algoritma Simetrik (*Symmetric Algorithms*), karena algoritma ini memakai suatu kunci yang serupa untuk melakukan prosedur enkripsi dan dekripsi data. Dalam melakukan proses enkripsi dan dekripsi, algoritma ini memakai suatu matriks persegi sebagai kunci yang diterapkan dan menerapkan aritmatika modulo.[10]

Dalam proses enkripsi, algoritma ini mengambil *plaintext* yang berurutan dan setiap huruf diberi nilai berupa angka seperti α =0 *b*=1,..., *z*=25. Untuk *m* =3, metode persamaan dapat didefinisikan sebagai berikut:

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26$$
$$C_1 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26 \quad (1)$$

Persamaan diatas memakai modulo 26 disebabkan *alphabet* yang akan dipakai pada saat melakukan enkripsi dan dekripsi sejumlah 26 karakter. Apabila persamaan diatas digunakan untuk citra digital berwarna (8 *bit*) maka Persamaan (1) memakai modul 256, sehingga Persamaan (1) menjadi :

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 256$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 256$$
$$C_1 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 256 \quad (2)$$

Persamaan (1) tanpa modular dapat diekspresikan dalam bentuk vektor kolom dan matriks sehingga menjadi :

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \quad (3)$$

DOI: 10.22236/teknoka.v%vi%i.4210
Seminar Nasional TEKNOKA ke - 4, Vol. 4, 2019
ISSN No. 2502-8782

atau sederhananya dapat menulis berupa C = KP, dimana P dan C adalah vektor kolom dengan panjang 3 baris, masing-masing baris mewakili *plaintext* dan *ciphertext*, dan K merupakan matriks 3 × 3, yang merupakan matriks kunci pada proses enkripsi. Untuk proses dekripsi memerlukan invers dari matriks K yang dibuat pada proses enkripsi. Invers matriks K (K-1) didefinisikan oleh persamaan K*K-1 = K-1*K = I, dimana I dinyatakan sebagai matriks identitas. Secara umum persaman tersebut dapat didefinisikan sebagai berikut:

Dalam proses Enkripsi:

$$C = E_k(P) = K_p P \quad (4)$$

Dalam proses Dekripsi:

$$P = D_k(C) = K^{-1}C = K^{-1}K_p = P \quad (5)$$

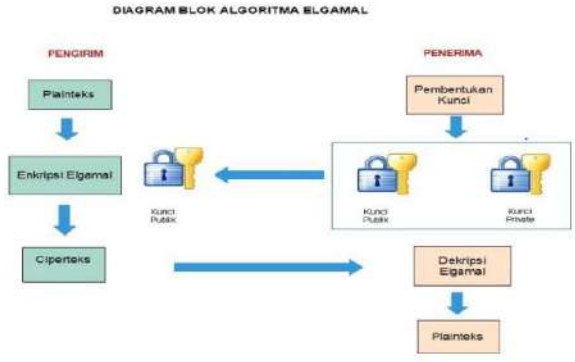
2.2 Kriptosistem ElGamal

Algoritma ElGamal dipublikasikan oleh Taher ElGamal pada tahun 1985. Hingga saat ini, algoritma ElGamal masih digunakan sebagai salah satu metode penyandian, contohnya pada penggunaan aplikasi PGP dan GnuPG yang terdapat pada keamanan email dan tanda tangan digital. Algoritma ElGamal tebentuk melalui 3 proses yakni proses pembentukan kunci,proses enkripsi data dan proses dekripsi data.

Algoritma ini menggunakan *chiper* blok, adalah suatu proses enkripsi pada blok-blok *chipertext*. Kemudian pada blok-blok *chipertext* dilakukan proses dekripsi, dan hasilnya digabungkan agar menjadi suatu pesan yang utuh dan mudah dimengerti. Dalam pembentukan Algoritma kriptografi ElGamal, Diperlukan bilangan prima *p* dan elemen primitif.[7]

Algoritma ElGamal memiliki *public key* berbentuk tiga pasang bilangan dan kunci rahasia berbentuk dua pasang bilangan. Algoritma ini memiliki kerugian terdapat pada pembentukan *chipertext*-nya yang memiliki ukuran dua kali lipat lebih besar dari pada *plaintext*-nya. Namun, Algoritma ElGamal miliki kelebihan pada proses enkripsi. Pada *plaintext* yang sama, algoritma ini menghasilkan *chipertext* yang berbeda-beda pada saat *plaintext* tersebut di enkripsi.

Hal tersebut disebabkan karena pengaruh dari suatu variabel yang ditetapkan secara acak saat proses enkripsi dilakukan . Pada Gambar 2.1 adalah diagram blok dari algoritma ElGamal.[6]



Gambar 2.1 *Skema Diagram Blok Algoritma Elgamal*

2.3 Domain Parameter Kurva Eliptik

Dalam pembahasan ini memuat tentang pembentukan domain parameter kurva eliptik atas F_p. Salah satu cara mengimplementasikan kriptografi kurva eliptik adalah dengan mempersiapkan parameter yang diperlukan oleh kriptosistem ElGamal. Domain parameter kurva eliptik atas F_p yang memenuhi standar SEC 2 didefinisikan sebagai berikut[11]:

$$T = (p, a, b, G, n, h) \quad (6)$$

Dimana:

p : bilangan prima
a, b : koefisien persamaan kurva eliptik
G : titik dasar yaitu elemen pembangunan grup kurva eliptik
n : order dari G yaitu bilangan bulat positif terkecil ɜ n. $G = 0$
h : kofaktor, $h = \#E/n$, $\#E$ adalah jumlah titik dalam grup Eliptik $E_p(a,b)$

2.4 Pembangkitan Kunci

Berdasarkan parameter yang sesuai pada standarisasi SEC 2, sebagian dari parameter yang terbentuk digunakan untuk membangkitkan kunci publik dan kunci privat tersebut. Untuk membangkitkan kunci tersebut dapat memakai perhitungan $Q = d.G$ yang sesuai berdasarkan aturan kurva elitpik. Jika kunci tersebut telah dibangkitkan, langkah selanjutnya yaitu proses enkripsi dan dekripsi citra. Algoritma pembangkit kunci ElGamal melalui kurva eliptik yakni[11] :

INPUT: Domain parameter $T = (p, a, b, G, n, h)$
OUTPUT: $K_{publik} = Q$, $K_{privat} = d$
Pilih $G = (X_1, Y_1)$sebagai titik pembangkit pada grup kurva eliptik $E(a, b)$
Pilih integer $d \in_R [1, n-1]$
Hitung $Q = d.G$
$K_{publik} = Q$, $K_{privat} = d$

2.5 Perancangan Sistem Enkripsi dan Dekripsi Citra

Dalam perancangan sistem enkripsi dan dekripsi, citra awal yang berwarna RGB (*Red Green Blue*) akan dienkripsi dengan menggunakan algoritma ElGamal. Pertama dalam melakukan proses enkripsi yaitu dengan menentukan persamaan kurva eliptik $y^2 = x^3 + \alpha x + b \pmod p$, dengan memasukkan nilai *a, b, p* untuk modulonya maka berdasarkan nilai tersebut dapat diperoleh beberapa titik – titik yang sesuai berdasarkan input yang dimasukkan. Nilai *a, b,* dan *p* akan mempengaruhi $E(F_p)$. Sesudah memperoleh beberapa titik tersebut, proses selanjutnya adalah mencari titik ketiga (X_3, Y_3), dimana titik ketiga ini diperoleh berdasarkan proses untuk membuat suatu kurva eliptik, hasil dari titik ketiga ini dapat digunakan sebagai kunci publik. Kunci publik yang digunakan berasal dari SEC (*Standards*

DOI: 10.22236/teknoka.v%vi%i.4210

ISSN No. 2502-8782

Efficient Cryptography) 2: *Recommended Elliptic Cuve Domain Parameter*.

Demikian juga untuk kunci privat yang digunakan berasal dari SEC 2. Setelah diperoleh kunci publik dan kunci privat dari SEC 2, selanjutnya memasukkan citra awal ke dalam sistem ini. Selanjutnya yaitu membangkitkan kunci (*generate key*), dimana kunci publik akan dikirim kepada penerima sedangkan kunci privat menjadi milik pribadi. Kemudian citra awal berwarna tersebut dibaca *pixel*-nya dalam bentuk *plaintext*. Setelah proses enkripsi citra awal tersebut berubah dan menghasilkan *chipertext*.

Citra awal (*M*) sebagai masukkan algoritma enkripsi kriptosistem ElGamal dengan kurva eliptik. Pengenkripsi memilih secara acak integer *k* dan menghitungnya. Berikut adalah algoritma yang digunakan dalam proses enkripsi[11]:

INPUT : Domain parameter $T = (p, a, b, G, n, h)$,
kunci publik Q, *plaintext* M
Output: Chipertext C1,C2
Pilih $k \epsilon_R [1, n-1]$
Hitung $C_1 = k.G$
Hitung $C2 = M + k.Q$
Chipertext C1,C2

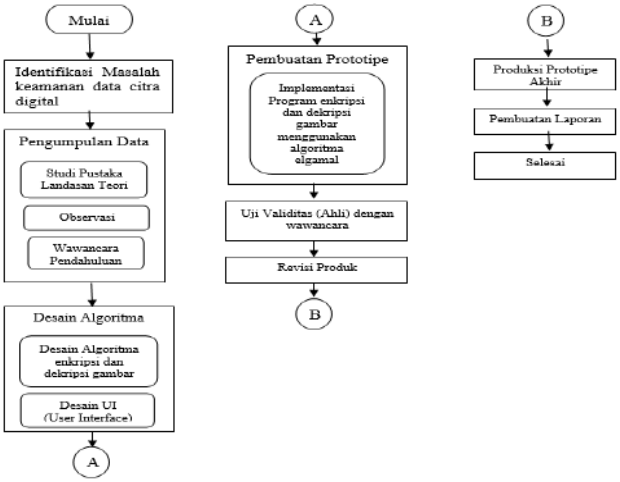
Dalam perancangan sistem dekripsi, akan mengubah kembali bentuk citra awal dari bentuk *chipertext* ke dalam bentuk *plaintext*. Citra dalam bentuk *chipertext* tersebut kemudian dimasukkan kunci privat yang bersumber dari SEC 2. Selanjutnya dilakukan proses dekripsi citra untuk mengembalikan citra ke dalam bentuk *plaintext*. Kemudian dilakukan proses pembacaan citra menjadi *pixel* dan menjadi citra asli. Berikut adalah algoritma yang digunakan dalam proses dekripsi[11]:

INPUT : Domain parameter $T = (p, a, b, G, n, h)$,
kunci privat d, *chipertext* $(C1, C2)$
OUTPUT: *plaintext M*
Hitung $M = C2 - d.C1$
plaintext M

3 METODOLOGI PENELITIAN

3.1 Diagram Alur Penelitian

Metodologi yang dipakai dalam penelitian ini menggunakan metodologi penelitian pengembangan (*Research and Development*). Metodologi penelitian dan pengembangan adalah suatu metode penelitian yang digunakan untuk menciptakan suatu produk tertentu seperti perangkat lunak, suatu alat dan komponen, dan menguji efektivitas dari produk yang telah dihasilkan tersebut. Pada gambar 3.1 adalah langkah-langkah penggunaan Metode R&D.



Gambar 3.1 *Langkah – Langkah Penggunaan Metode R&D*

3.2 Penjelasan Diagram Alur Metodologi Penelitian

Dalam sub bab ini, penulis menjelaskan secara singkat mengenai diagram alir penelitian yang ditunjukan pada Gambar 3.1.

Pada Tahap Identifikasi Masalah Keamanan Data Citra Digital. Tahap ini akan mengidentifikasi masalah pada keamanan data citra yang ada di PT.Puninar Yusen Logistics Indonesia, serta masalah yang dihadapi oleh karyawan yaitu tentang keamanan data gambar yang ada di perusahaan. Dan dari masalah tersebut terdapat potensi apa yang dapat dikembangkan untuk mengatasi masalah yang ada.

Pada tahap pengumpulan data, penulis menggunakan beberapa metode atau teknik yang digunakan dalam mengumpulkan data. Adapun metode yang digunakan penulis dalam pengumpulan data adalah:

a. Studi Pustaka Landasan Teori
Penulis mengumpulkan data-data menggunakan buku dan jurnal yang berhubungan dengan penelitian.
b. Observasi
Metode ini dilakukan dengan mengamati dan melihat langsung Aplikasi keamanan data yang digunakan di PT.Puninar Yusen Logistics Indonesia.
c. Wawancara Pendahuluan
Sebuah proses tanya-jawab yang dilakukan secara langsung dengan lisan yang ditunjukan kepada Kepala Departemen IT dari PT Puninar Yusen Logistics Indonesia, bertujuan untuk menentukan apakah Aplikasi keamanan data yang penulis ajukan sekiranya cocok dan dapat di terapkan di PT.Puninar Yusen Logistics Indonesia.

Pada Tahap Desain Algoritma, penulis melakukan desain algoritma enkripsi dan dekripsi gambar untuk bagian komponen utama dalam pembuatan aplikasi enkripsi dan dekripsi menggunakan algoritma ElGamal. Dan desain *User Interface* untuk memberikan gambaran tentang sistem yang akan dibangun dan hasilnya sesuai dengan kebutuhan. Dengan memperhatikan desain tampilan

DOI: 10.22236/teknoka.v%vi%i.4210 *ISSN No. 2502-8782*

sehingga mempermudah pengguna dalam menggunakan aplikasi ini.

Pada Tahap Pembuatan Prototipe, penulis melakukan implementasi program enkripsi dan dekripsi gambar menggunakan algoritma ElGamal. Desain yang sebelumnya dirancang diimplementasikan pada sebuah aplikasi berbasis *mobile Android* Studio yang digunakan dalam pembuatan aplikasi ini. Dilakukan juga tahap validasi produk yang dilakukan oleh narasumber yang sudah berpengalaman untuk menilai aplikasi yang sudah dirancang tersebut. Validasi dilakukan untuk mengetahui kelemahan dan kelebihan aplikasi untuk diperbaiki.

Setelah melakukan validasi pembuatan produksi prototipe akhir Aplikasi enkripsi dan dekripsi gambar menggunakan algoritma ElGamal dilakukan.

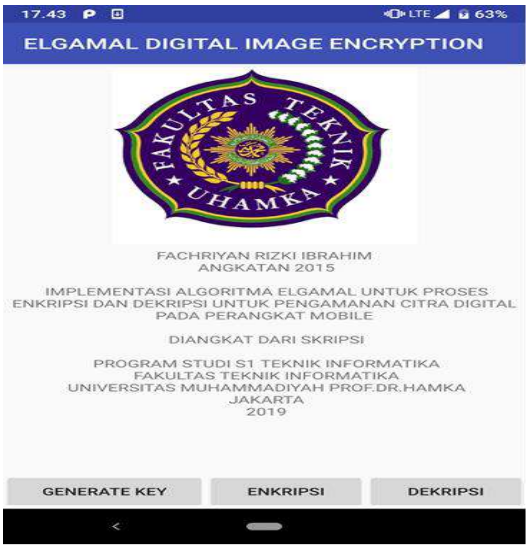
Pada Tahap pembuatan laporan penulis menjelaskan secara keseluruhan penelitian yang telah dirancang dan diuji.

4 HASIL DAN PEMBAHASAN

Sistem akan diuji untuk mengetahui apakah proses enkripsi dan dekripsi citra dapat berjalan dengan baik. Pada penelitian ini, aplikasi dibuat pada perangkat *mobile* dengan sistem operasi *Android* menggunakan bahasa pemrograman *Java*. *Software* yang digunakan adalah *Android Studio*. Format gambar yang diuji adalah .jpg, .bmp, .png, dan .gif dengan resolusi maksimal 1500x1500 *pixel* Aplikasi ini memiliki 4 halaman, yaitu : Home, Generate Key, Enkripsi, dan Dekripsi.

4.1. *Interface* Halaman *Home*

Interface halaman *Home* dapat dilihat pada gambar 4.1.

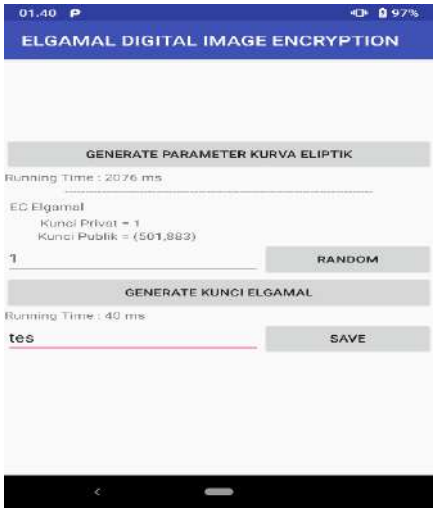


Gambar 4.1 *Interface Halaman Home*

Halaman *Home* merupakan halaman utama yang berisikan judul aplikasi, logo universitas, identitas pembuat aplikasi , tombol *generate key* , enkripsi , dan dekripsi.

4.2 Interface Halaman Generate Key

Interface halaman *Generate Key* dapat dilihat pada gambar 4.2.

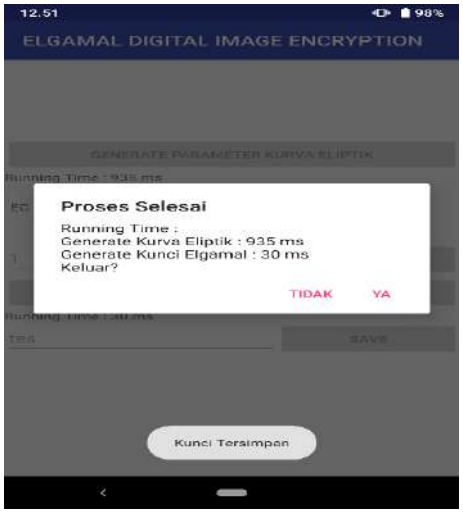


Gambar 4.2 *Interface halaman Generate Key*

Halaman *Generate Key* merupakan halaman yang memuat proses pembangkitan kunci publik dan kunci privat yang akan digunakan untuk melakukan proses enkripsi dan dekripsi. Proses pada halaman ini akan membentuk suatu parameter kurva eliptik, yaitu parameter yang dihasilkan untuk membentuk kunci publik algoritma ElGamal. Untuk kunci privat pengguna bisa langsung menentukan nilai yang diinginkan atau menentukan nilai secara acak dengan tombol *random*.

Setelah selesai menentukan nilai untuk kunci privat dan kunci publik pengguna menekan tombol *Generate* Kunci ElGamal, dan memasukkan nama untuk kunci privat dan kunci publik. Setelah selesai pengguna menekan tombol *save* untuk menyimpan kunci publik dan kunci privat yang telah di *input*.

Setelah itu akan keluar notifikasi yang menyatakan proses *generate key* selesai. Tampilan notifikasi proses *generate key* selesai dapat dilihat pada gambar 4.3



Gambar 4.3 *Notifikasi Proses Generate Key Selesai*

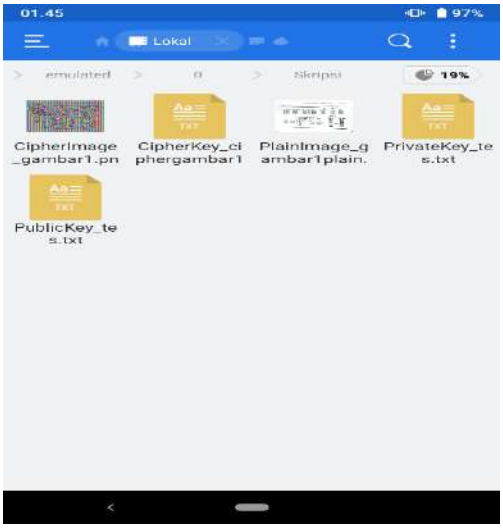
Pada notifikasi proses *generate key* terdapat keterangan *Real Running Time* yang merupakan lama

DOI: 10.22236/teknoka.v%vi%i.4210

ISSN No. 2502-8782

waktu untuk pembuatan kurva eliptik dan kunci algoritma ElGamal.

Setelah notifikasi telah ditampilkan dan kunci telah dibuat maka secara otomatis kunci yang telah dibuat akan tersimpan di *memory internal smartphone* dengan nama *folder* "Skripsi". Tampilan *folder* penyimpanan kunci dapat dilihat pada gambar 4.4

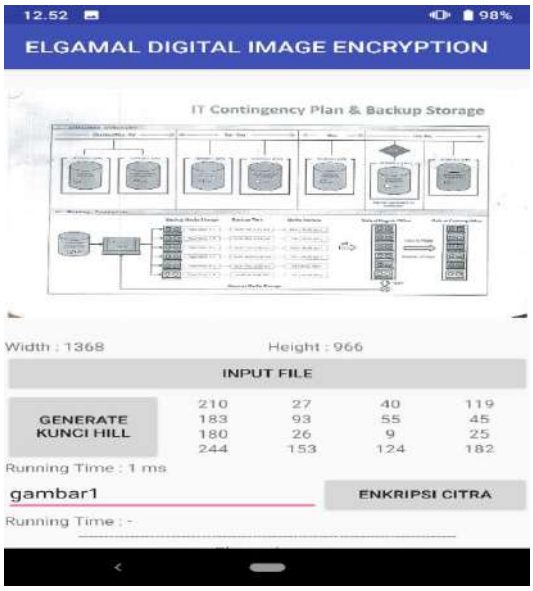


Gambar 4.4 *Folder Penyimpanan Kunci*

Pada *folder* penyimpanan kunci terdapat kunci privat, kunci publik, *chiperkey*, *cipherimage* dan *plainimage.*

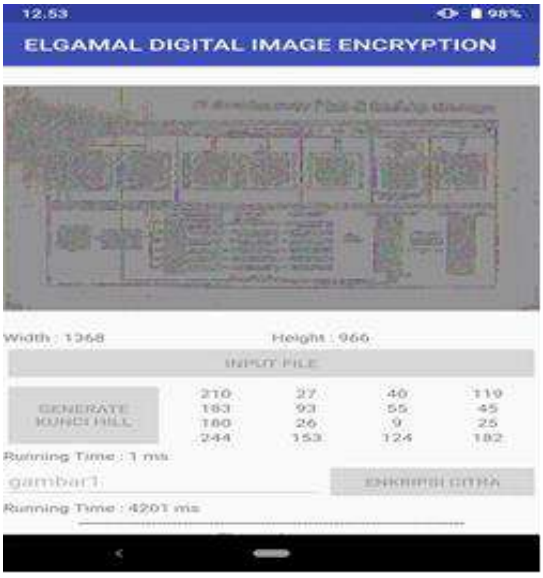
4.3 Interface Halaman Enkripsi

Interface halaman sebelum citra dienkripsi dapat dilihat pada gambar 4.5.



Gambar 4.5 *Tampilan Sebelum Citra Dienkripsi*

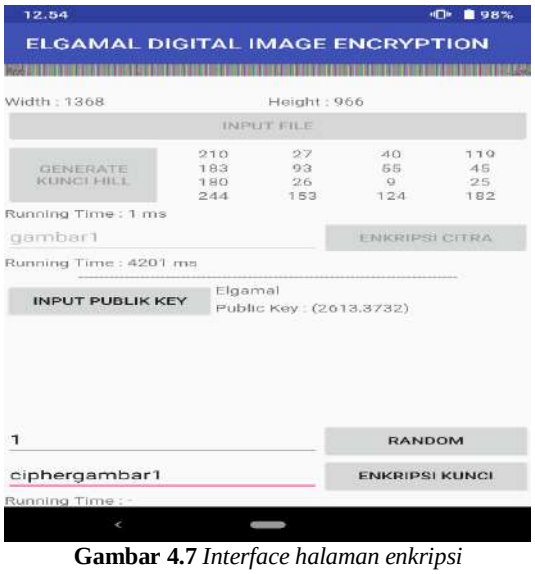
Halaman enkripsi merupakan halaman yang memuat proses pengenkripsian citra digital. Di halaman ini *file* citra dan kunci *Hill Cipher* dienkripsi. Citra digital dienkripsi menjadi *cipherimage* dan kunci *Hill Cipher* dienkripsi menjadi *cipherkey*. Citra dienkripsi menggunakan kunci dari *Hill Cipher*, lalu kunci dari *Hill Cipher* tersebut dienkripsi menggunakan kunci publik yang telah dibangkitkan pada halaman *Generate Key* dengan algoritma ElGamal. Pengguna lalu memasukkan nama yang akan digunakan untuk *cipherimage* dan menekan tombol enkripsi citra. Sedangkan untuk *Interface* setelah citra di enkripsi dapat dilihat pada gambar 4.6.



Gambar 4.6 *Interface Setelah Citra Dienkripsi*

Pada gambar 4.6 citra awal yang masih utuh dienkripsi menjadi *cipherimage* agar informasi di dalam citra tersebut tidak dapat dilihat.

Tampilan halaman enkripsi dapat dilihat pada gambar 4.7



Gambar 4.7 *Interface halaman enkripsi*

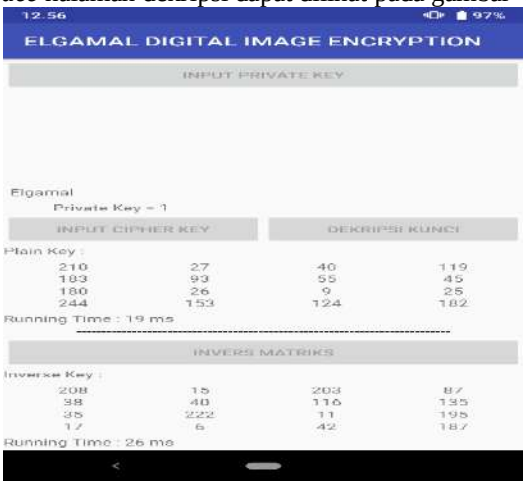
Setelah citra telah berhasil di enkripsi pengguna menekan tombol *Input* publik *Key* dan memasukkan kunci publik yang telah tersimpan pada *folder* skripsi. Pengguna lalu dapat menentukan bilangan acak *r* dengan memasukkan nilai yang diinginkan atau menentukan nilai secara acak dengan menekan tombol *random*. Setelah bilangan acak *r* di tentukan makan penggun dapat memasukkan nama yang digunakan untuk *cipherkey* dengan menekan tombol enkripsi kunci. Sistem akan menampilkan notifikasi proses

DOI: 10.22236/teknoka.v%vi%i.4210
Seminar Nasional TEKNOKA ke - 4, Vol. 4, 2019
ISSN No. 2502-8782

selesai dan menampilkan *Running Time* dari *Generate* matriks, Enkripsi Citra, dan Enkrips Kunci. *File cipherimage* dan *cipherkey* yang telah dibuat tersimpan didalam *folder* "Skripsi".

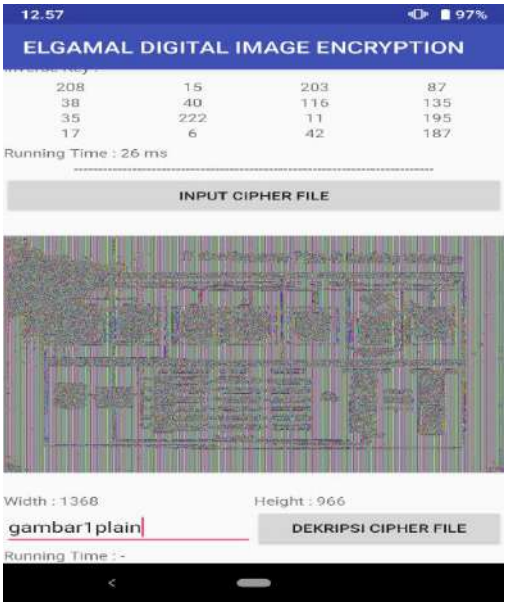
4.4 Interface Halaman Dekripsi

Interface halaman dekripsi dapat dilihat pada gambar 4.8.



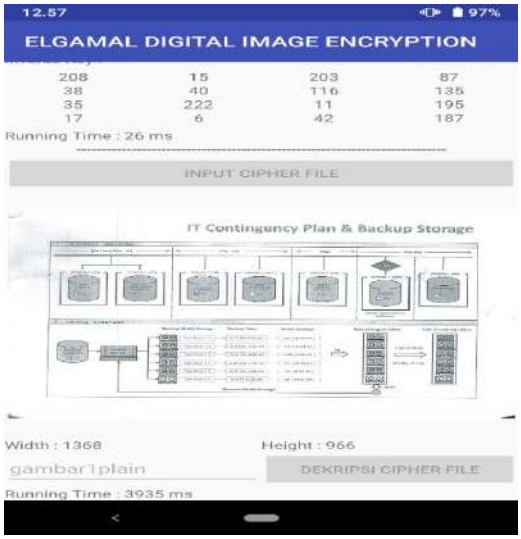
Gambar 4.8 *Tampilan halaman Dekripsi*

Halaman dekripsi merupakan halaman yang memuat proses pendekripsian citra digital. Pada halaman ini kunci privat dan *cipherkey* diinputkan. Pengguna menekan tombol Dekripsi Kunci, kemudian *cipherkey* didekripsi menjadi *plain key* menggunakan kunci privat dengan algoritma ElGamal. Lalu pengguna menekan tombol Invers Matriks kemudian *plain key* yang telah didapat dicari invers matriks dari *plain key*, yang kemudian digunakan untuk mendekripsi *cipherimage* menjadi *plainimage* atau citra awal.
Tampilan sebelum citra didekripsi dapat dilihat pada gambar 4.9.



Gambar 4.9 *Tampilan Sebelum Citra Didekripsi*

Setelah invers matriks dari *plainkey* didapatkan pengguna menekan tombol *Input Cipher File* lalu pengguna memasukkan *cipherimage* yang telah disimpan pad *folder* Skripsi. Kemudian pengguna memasukkan nama yang akan digunakan untuk *plainimage* atau citra awal. Setelah nama dimasukkan pengguna lalu menekan tombol Dekripsi *Cipher File*, dan *Cipherimage* akan didekripsi menjadi *plainimage.*
Tampilan setelah citra didekripsi dapat dilihat pada gambar 4.10.



Gambar 4.10 *Tampilan Setelah Citra Didekripsi*

Pada gambar 4.10 adalah tampilan setelah citra didekripsi. Citra yang sebelumnya dienkripsi dan berubah menjadi *cipherimage* didekripsi agar citra tersebut kembali ke bentuk awal dan informasi didalam citra tersebut bisa terlihat.

4.5 Pengujian Aplikasi

Pengujian aplikasi yang dilakukan menggunakan metode *black box* untuk memeriksa apakah setiap komponen yang telah dibuat di dalam sistem telah bekerja dan proses sistem ini dapat dilihat pada tabel 4.1.

Tabel 4.1(a) *Tabel pengujian Aplikas ElGamal Digital Encryption*

Menu yang diuji	Pengujian	Hasil	Keterangan
Home	Memilih *button*	*Button* dapat di klik dan berpindah *scene* sesuai nama *button.*	Berhasil
Generate Key	Membangkitkan parameter kurva eliptik	Parameter kurva eliptik dapat dibangkitkan dan sistem dapat menampilkan *Real Running Time* saat para meter dibangkitkan	Berhasil
	Random	Sistem dapat menentukan angka secara acak	Berhasil
	Membangkitkan Kunci ElGamal	Kunci publik dan kunci privat ElGamal dapat dibangkitkan	Berhasil
	Save	Sistem dapat menyimpan kunci ElGamal yang telah dibangkitkan dan dapat menampilkan notifikasi proses *generate key* selesai	Berhasil
	Pindah *scene*	Setelah kunci tersimpan dan notifikasi ditampilkan muncul opsi keluar, dan ketika di klik dapat kembali ke menu *Home*	Berhasil

DOI: 10.22236/teknoka.v%vi%i.4210
Seminar Nasional TEKNOKA ke - 4, Vol. 4, 2019
ISSN No. 2502-8782

Tabel 4.1(b) *Tabel pengujian Aplikasi ElGamal Digital Encryption*

Menu yang diuji	Pengujian	Hasil	Keterangan
Enkripsi	*Input File*	Sistem dapat menerima masukkan berupa *file* citra digital dengan ekstensi .jpg, .png, .bmp, dan .gif dengan resolusi maksimal 1500x1500 *pixel*	Berhasil
	Generate Hill	Sistem dapat membangkitkan kunci *hill* dengan matriks angka secara *random*	Berhasil
	Enkripsi Citra	Sistem dapat mengenkripsi citra yang di *input* menjadi *cipherimage*	Berhasil
	Input Publik *Key*	Sistem dapat membaca masukan berupa kunci publik ElGamal	Berhasil
	Random	Sistem dapat menentukan angka secara acak	Berhasil
	Enkripsi Kunci	Sistem dapat melakukan penyimpanan file *cipherimage* dan *cipherkey* yang telah dibuat serta dapat menampilkan notifikasi proses enkripsi selesai	Berhasil
	Pindah *scene*	Setelah kunci tersimpan dan notifikasi ditampilkan muncul opsi keluar, dan ketika di klik dapat kembali ke menu *Home*	Berhasil

Tabel 4.2(c) *Tabel pengujian Aplikasi ElGamal Digital Encryption*

Menu yang diuji	Pengujian	Hasil	Keterangan
Dekripsi	*Input Private Key*	Sistem dapat menerima masukkan berupa *file* kunci privat yang telah dibuat	Berhasil
	Input Cipher Key	Sistem dapat menerima masukkan berupa *file cipherkey* yang telah dibuat	Berhasil
	Dekripsi Kunci	Sistem dapat melakukan proses dekripsi kunci dan menampilkan *plainkey* dari *cipherkey* yang telah dibuat	Berhasil
	Invers Matriks	Sistem dapat melakukan proses invers matriks dari *plainkey* yang telah ditampilkan	Berhasil
	Input Cipher File	Sistem dapat menerima dan menampilkan masukkan berupa file *cipherimage* yang telah dibuat	Berhasil
	Dekripsi *Cipher File*	Sistem dapat melakukan proses pendekripsian file *cipherimage* menjadi *plainimage* dan menampilkan notifikasi proses dekripsi selesai	Berhasil
	Pindah *scene*	Setelah citra berhasil didekripsi muncul opsi keluar, dan ketika di klik dapat kembali ke menu *Home*	Berhasil

5 SIMPULAN

Berdasarkan hasil dari penelitian ini, didapatkan kesimpulan bahwa:

1. Pengamanan Citra digital dilakukan dengan menggunakan Algoritma ElGamal dengan menggabungkan dua buah kunci yaitu kunci publik dan kunci privat.
2. Citra digital yang dapat dienkripsi adalah citra digital dengan format .jpg, .bmp, .png, dan .gif dengan resolusi maksimal 1500x1500 *pixel*.
3. Algoritma ElGamal dapat diimplementasikan dan diterapkan dalam pengamanan citra digital untuk perangkat *mobile*.

KEPUSTAKAAN

[1] Triase, *Kriptografi Elgamal Menggunakan Metode Mersenne*, Jurnal Ilmiah Integritas Volume I, No.4:2-3, Desember 2015.

[2] Mukhtar, Harun, *Kriptografi Untuk Keamanan Data*, Yogyakarta: Deepublish, 2018.

[3] Irawati, Indrarini Dyah, *Jaringan Komputer dan Data Lanjut*, Yogyakarta: Deepublish, 2018.

[4] Rusri Yanti, Neti, *Implementasi Algoritma Data Encryption Standard pada penyandian Record Database*, Jurnal Sains & Informatika Volume II, No.1:23-32, Maret 2018.

[5] Chandra, *Keamanan Data Dengan Metode Kriptografi Kunci Publik*, Jurnal TIMES Volume V, No.2:11-15, 2016.

[6] Widarma, Andi, *Kombinasi Algoritma AES, RC4 dan ElGamal Dalam Skema Hybird Untuk Keamanan Data*, CESS (Journal Of Computer Engineering System And Science) Volume I, No.1:1-8, Januari 2016.

[7] Agung Bagus, I Gusti, Sianipar Rismon H, dan Wiryajati, I Ketut., *Teknik Steganografi Menggunakan Transformasi Slant Dengan Algoritma Enkripsi Elgamal*, Dielektrika Volume I, No.1:6-15, Februari 2014.

[8] Enterprise, Jubilee, *Java Untuk Pemula*, Jakarta: PT Elex Media Komputindo, 2014.

[9] Suryana, Dayat, *Belajar Android Studio*, Bandung: Dayat Suryana Independent, 2018.

[10] Supriyanto, *Implementasi Hill Cipher pada Citra Menggunakan Koefisien Binomial Sebagai Matriks Kunci*, Seminar Nasional Informatika, No.1:284-291, November 2015.

[11] Budi Utomo Daryono, Winda Setyawati Dian, dan Romadhoni F.R Gestihayu, *Kriptografi Eliptik ElGamal Untuk Proses Enkripsi-Dekripsi Citra Digital berwarna*, Seminar Nasional Matematika Volume I, No.1: 373-383. 2014.

[12] Pudjo Widodo Prabowo, *Menggunakan UML*, Bandung:Informatika, 2012.

[13] Parmadi, Binantara, *Implementasi Algoritma Kriptografi ElGamal pada data Text*, Journal of Information and Technology Volume V, No.1:1-5, Juni 2017.

[14] Taufiq Tamam, M. , Dwiono Wakhyu, Hartanto Tri, *Penerapan Algoritma Kriptografi ElGamal Untuk pengamanan file citra*, Jurnal EECCIS Volume I, No.1:8-11, Juni 2010.

DOI: 10.22236/teknoka.v%vi%i.4210

ISSN No. 2502-8782