e-ISSN : 2722-4368

Penerapan Enkripsi Menggunakan Metode Elgamal guna Meningkatkan Keamanan Data Text dan Gambar

Fahri Husaini[1)], Akim M.H Pardede[2)], Imeldawaty Gultom[3)]
[123]STMIK Kaputama
Jl.Veteran No. 4A-9A, Binjai, Sumatera Utara
e-mail: fahrihusaini044@gmail.com

Abstract- *Data security is very important in maintaining the confidentiality of information, especially those containing sensitive information whose contents should only be known by the entitled people. especially if the transmission is done through a public network, if the data is not secured beforehand, it will be very easy to be intercepted and the contents of the information known by irresponsible people. One of the methods used to secure data is to use a cryptographic system, namely by providing the information content (plaintext) into content that is not understood through the encryption process, and to retrieve the original information, a description process is carried out, accompanied by using the correct key. Therefore, the author recommends the Elgamal algorithm to be able to provide security for text data. The reason the author uses the ElGamal algorithm is that the ElGamal algorithm is part of asymmetric cryptography where the formation of one of the keys uses prime numbers and focuses on the strength of the key in solving discrete logarithm problems.*

Keywords: *Image, Cryptography, Text, ElGamal*

Abstrak- Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak bertanggung jawab.Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyediakan isi informasi (plaintext) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi, dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi, disertai dengan menggunakan kunci yang benar. Oleh karena itupenulis merekomendasikan algoritma Elgamal untuk dapat memberikan keamanan pada Data text. Alasan Penulis menggunakan algoritma ElGamal adalah Algoritma ElGamal merupakan bagian dari kriptografi asimetris yang pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit

Kata Kunci : Citra, Kriptografi, Text, ElGamal

PENDAHULUAN

Keamanan data merupakan hal yang sangat penting dalam menjagakerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak bertanggung jawab.

Saat ini pencurian data melalui plagiasi dan modifikasi sering ditemui dalam kehidupan digital. Dokumen yang banyak digunakan adalah dokumen dengan ekstensi docx. Hal ini dikarenakan dokumen dengan ekstensi.docx merupakan salah satu dokumen yang mudah dalam proses pembuatan serta penyimpanannya Untuk menjaga kerahasiaan, integritas, pengenalan identitas pengirim dan pencegahan penyangkalan pengiriman datadokumen, maka diperlukan sebuah alat bantu untuk melindungidokumen tersebut. Hal ini menjadimasalah utama dalam persaingan dunia bisnis. Oleh karena itu untuk menjaga integritas data tersebut dibutuhkan sebuah sistem keamanan berupa penyandian atau pengkodean data sebelum proses pengiriman dilakukan, yang bertujuan untuk

mengamankan data penting yang bersifat rahasia agar tidak dengan mudah dibaca dan diubahisi dari pesan tersebutoleh pihak yang tidak berkepentingan

Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyediakan isi informasi (plaintext) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi, dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi, disertai dengan menggunakan kunci yang benar.

Oleh karena itu penulis merekomendasikan algoritma ElGamal untuk dapat memberikan keamanan pada Data text dan gambar png. Alasan Penulis menggunakan algoritma ElGamal adalah Algoritma ElGamal merupakan bagian dari kriptografi asimetris yang pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit. Dengan memanfaatkan bilangan prima yang besar serta masalah logaritma diskrit yang cukup menyulitkan, maka keamanan kuncinya lebih terjamin. Proses enkripsi ElGamal dari plaintext ke dalam bentuk ciphertext didahului pembentukan kunci oleh penerima pesan, dua macam pasangan kunci yaitu kunci public dan kunci private. Kunci public untuk disebarluaskan sedangkan kunci private untuk diri sendiri. Untuk membuat sebuah pesan rahasia dalam bentuk ciphertext, pesan rahasia harus dikonversikan terlebih dahulu dalam bilangan bulat kemudian dikodekan berdasarkan kode ASCII(American Standart for Information Interchange). Pesan dalam bentuk ciphertext didekripsi menggunakan kunci private untuk dikembalikan menjadi pesan yang sebenarnya. Sehingga Kriptografi ElGamal melindungi pesan rahasia dengan aman.

METODOLOGI

2.1 Penelitian Terdahulu

Penelitian ini didasari dari beberapa acuan untuk dijadikan sumber referensi sebagai berikut“Pengiriman pesan dengan algoritma kriptografi ElGamal”.Metodologi yang digunakan dalam melakukan penelitian ini menggunakan pengumpulan dokumen, studi pustaka dan eksperimen. Pengumpulan dokumen selayaknya guna mendapatkan dokumen input untuk diproses menghasilkan output serta dokumen untuk kelancaran penelitian. Dokumen yang digunakan pada penelitian ini seperti dokumen proses analisa sistem, desain proses, pembuatan kode program dan aplikasi sampai dengan pengujian aplikasi menggunakan Metode ElGamal. Studi pustaka bermanfaat mendapatkan referensi penelitian yang telah dilakukan sebelumnya yang berhubungan dengan penelitian saat ini dilaksanakan untuk diterapkan metode tersebut dalam penelitian. Eksperimen dilakukan dengan memasukan plaintext secara acak (random) dan disimpan ke dalam File Teks (TXT) untuk diproses dengan Metode ElGamal baik saat enkripsi maupun dekripsi serta membandingkan hasil dekripsi dengan isi dokumen asal plaintext(Fajrin et al., 2019)

Analisa algoritma ElGamal dalam penyediaan data sebagai keamanan database” Penelitian ini bertujuan untuk mengamankan sebuah data, Algoritma ini pada umumnya digunakan untuk digital signature, kemudian dimodifikasi sehingga bisa digunakan untuk enkripsi dan dekripsi. Pada proses ekripsi database Pesan tersebut sebelumnya harus dikonversikan dalam kode ASCII terlebih dahulu karena algoritma ElGamal menggunakan bilangan bulat dalam perhitungannya. Pesan yang dienkripsi tersebut kemudian dikirimkan kepada penerima pesan yang mempunyai kunci rahasia untuk mendekripsikan pesan yang telah dienkripsi. Keamanan algoritma ElGamal secara teknis terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sulit untuk dipecahkan. Dengan menggunakan metode Algoritma ElGamal, proses enkripsi file database yang akan di enkripsi adalah isi data pada tabel (cipherteks), file database masih dapat dibuka dan dilihat akan tetapi isi data pada tabel tidak bisa dibaca, kemudian proses dekripsi untuk mengembalikan file database yang telah di enkripsi kembali menjadi file awal (plainteks)(Sari et al., 2018)

Pembangkitan kunci pada algoritma asimetris ElGamal untuk meningkatkan keamanan data bertipe DOCX. Penelitian ini bertujuan untuk mengamankan sebuah pesan bertipe docx. Metode ini menggunakan pembangkitan kunci untuk menghasilkan kombinasi kunci yang variatif. Kunci yang dihasilkan berupa kunci privat, kunci public, bilangan prima serta bilangan acak. Berdasarkan hasil percobaan, proses pembangkitan kunci pada algoritma ElGamal mampu mengacak isi pesan

berekstensi .docx secara aman. Hal ini terbukti dengan percobaan menggunakan beberapa kombinasi bilangan prima dan kunci private terhadap data yang sudah dienkripsi, kunci belum mampu terpecahkan. Pengujian penyerangan dilakukan dalam waktu lebih dari 15 jam, namun algoritma ElGamal belum mampu terpecahkan. Selain itu, sebagai dampak dari pengujian terhadap file, menghasilkan perbedaan ukuran file asli dengan file yang telah dienkripsi ratarata 7 kali lipat. Perubahan ukuran tersebut tidak berpengaruh, sebab file akan kembali ke ukuran semula setelah proses dekripsi. Dari segi keamanan, penggunaan algoritma ElGamal ini dinyatakan cukup kuat sebagai alternatif untuk membantu meningkatkan keamanan data .docx(Karima & Saputro, 2016).

2.2 Kriptografi

Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem Kriptografi (Cryptosystem) adalah kumpulan dari fungsi enkripsi dan dekripsi yang berkoresponden terhadap kunci enkripsi dan dekripsi[3]. Menurut Katz, kriptografi adalah studi ilmiah atau teknik untuk mengamankan informasi digital, transaksi dan komputasi yang terdistribusi. (Gunawan, 2018 : 125).

Kriptografi bertujuan untuk memberikan layanan keamanan sebagai berikut :

1. Kerahasiaan (*Confidentiality*)
   Informasi dirahasiakan dari semua pihak yang tidak berwenang.
2. Keutuhan Data (*Integrity*)
   Pesan tidak berubah dalam proses pengiriman hingga pesan diterima oleh si penerima.
3. Autentikasi (*Message Autentication*)
   Kepastian terhadap identitas yang terlibat dan keaslian sumber data.
4. Nirpenyangkalan (*Nonrepudiation*)

Setiap entitas yang berkomunikasi tidak dapat menolak atau menyangkal atas data yang telah dikirim atau diterima. (Gunawan, 2018 : 125).

2.3 Keamanan

Keamanan adalah keadaan bebas dari bahaya. Istilah ini dapat digunakan dengan hubungan kepada kejahatan, dan segala bentuk kecelakaan. Keamanan merupakan topik yang luas termasuk keamanan nasional terhadap seorang teroris, keamanan komputer terhadap hacker, keamanan rumah terhadap maling dan penyusup lainnya, keamanan financial terhadap kehancuran ekonomi dan banyak situasi berhubungan lainnya. Host Komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada host yang tidak berhubungan kemana-mana. Dengan mengendalikan network security resiko tersebut dapat dikurangi. (Santoso dan Fakhriza, 2018 : 48).

2.4 Algoritma ElGamal

Algoritma ElGamal ditemukan pada tahun 1985 oleh ilmuwan Mesiryaitu Taher ElGamal. Algoritma ElGamal merupakan algoritma berdasarkan konsep kunci publik.Algoritma ini pada umumnya digunakan untuk digital signature, namun kemudian dimodifikasi sehingga bisa digunakan untuk enkripsi dan dekripsi.

Algoritma kriptografi kunci publik ElGamal merupakan algoritma blok chipper yaitu algoritma yang melakukan proses enkripsi pada blok-blok plainteks yang kemudian menghasilkan blok-blok chippertext, yang nantinya blok-blok chippertext tersebut akan didekripsi kembali dan hasilnya kemudian digabungkan menjadi plainteks semula.

Keamanan algoritma ElGamal terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah logarithma ini menjadi sulit untuk dipecahkan.Algoritma ini memiliki kelebihan yaitu pembangkitan kunci yang menggunakan logaritma diskrit dan metode enkripsi dekripsi yang menggunakan proses komputasi yang besar sehingga hasil enkripsinya berukuran dua kali dari ukuran semula.

Kekurangan nalgoritma ini adalah membutuhkan resource yang besar karena chippertext yang dihasilkan dua kali panjang plaintext serta membutuhkan processor yang mampu untuk melakukan komputasi yang besaruntuk perhitung anlogaritma perpangkatan besar.Untuk proses dekripsi, algoritma ini membutuhkan waktu yang lebih lama karena kompleksitas proses dekripsinya yang

rumit. Dibutuhkan dua kali komputasi karena ukuran chipperteks yang lebih besar dibandingkan plainteksnya.

HASIL DAN PEMBAHASAN

3.1 Perhitungan

Untuk dapat membuktikan keberhasilan pada suatu metode yang diterapkan ke dalam sebuah aplikasi, maka diperlukan sebuah perhitungan manual. Langkah- langkah metode ElGamal untuk enkrip dapat dilihat sebagai berikut :

Dari beberapa percobaan yang sudah dilakukan, berikut diuraikan simulasi perhitungan manual proses enkripsi algoritma *ElGamal* dengan rincian sebagai berikut :

Plaintext(*m*) :ABCDEF
Bilangan acak prima(*p*) :2273
Bilangan acak(*g*) :3
Kunci private(*x*) :243
Kunci public (*y*) :3243 mod 2273 = 461
Bilangan acak pengirim(*k*) : k =762

a. Proses Enkripsi

Sebelum melakukan proses enkripsi, file asli (*plaintext*) harus diubah kedalam nilai decimal ASCII terlebih dahulu, dengan A = 65, B = 66, C = 67, D = 68, E = 69, F = 70. Adapun simulasi perhitungan enkripsi algoritma *ElGamal.*

No	Karakter ASCII	Proses		Hasil	
				A	B
1	A	$a = g^k \bmod p$ $= 3^{762} \bmod 2273$ $= 613$	$b = y^k m \bmod p$ $= 461^{762}.65 \bmod 2273$ $= 1001$	613	1003
2	B	$a = g^k \bmod p$ $= 3^{762} \bmod 2273$ $= 613$	$b = y^k m \bmod p$ $= 461^{762}.66 \bmod 2273$ $= 1508$	613	1508
3	C	$a = g^k \bmod p$ $= 3^{762} \bmod 2273$ $= 613$	$b = y^k m \bmod p$ $= 461^{762}.67 \bmod 2273$ $= 2013$	613	2013
4	D	$a = g^k \bmod p$ $= 3^{762} \bmod 2273$ $= 613$	$b = y^k m \bmod p$ $= 461^{762}.68 \bmod 2273$ $= 245$	613	245
5	E	$a = g^k \bmod p$ $= 3^{762} \bmod 2273$ $= 613$	$b = y^k m \bmod p$ $= 461^{762}.69 \bmod 2273$ $= 750$	613	750
6	F	$a = g^k \bmod p$ $= 3^{762} \bmod 2273$ $= 613$	$b = y^k m \bmod p$ $= 461^{762}.70 \bmod 2273$ $= 1255$	613	1255

Nilai karakter tersebut merupakan hasil proses enkripsi yang kemudian akan digunakan dalam proses dekripsi file.

b. Proses Deskripsi

Adapun proses perhitungan nilai file hasil enkripsi *ciphertext* menjadi file asli *plaintext* (m) sesuai pada table 2 berikut ini.

Dekripsi M1 (613, 1003)

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

$= 613^{2029} \bmod 2273 = 2264$

$m1 = b/a^x \bmod p$

e-ISSN : 2722-4368

$= b(a^x)^{-1} \bmod p$
$= 1003 \cdot 2264 \bmod 2273$
$= 65$

Dekripsi M2 (613, 1508)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$= 613^{2029} \bmod 2273 = 2264$

m1 $= b/a^x \bmod p$
$= b(a^x)^{-1} \bmod p$
$= 1508 \cdot 2264 \bmod 2273$
$= 66$

Dekripsi M3 (613, 2013)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$= 613^{2029} \bmod 2273 = 2264$

m1 $= b/a^x \bmod p$
$= b(a^x)^{-1} \bmod p$
$= 2013 \cdot 2264 \bmod 2273$
$= 67$

Dekripsi M4 (613, 245)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$= 613^{2029} \bmod 2273 = 2264$

m1 $= b/a^x \bmod p$
$= b(a^x)^{-1} \bmod p$
$= 245 \cdot 2264 \bmod 2273$
$= 68$

Dekripsi M5 (613, 750)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$= 613^{2029} \bmod 2273 = 2264$

m1 $= b/a^x \bmod p$
$= b(a^x)^{-1} \bmod p$
$= 750 \cdot 2264 \bmod 2273$
$= 69$

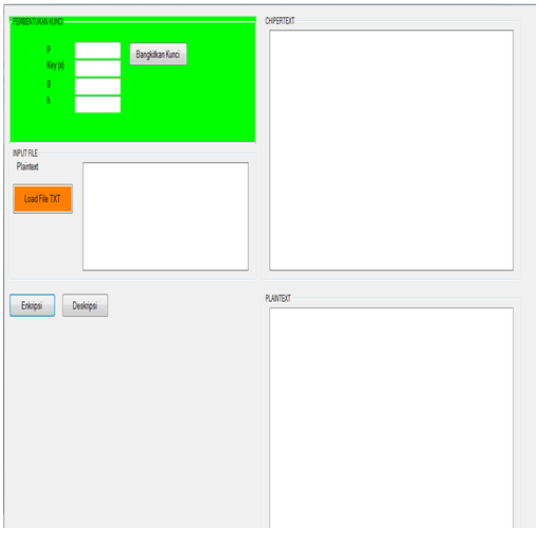
Dekripsi M6 (613, 1255)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$= 613^{2029} \bmod 2273 = 2264$

m1 $= b/a^x \bmod p$
$= b(a^x)^{-1} \bmod p$
$= 1255 \cdot 2264 \bmod 2273$
$= 70$

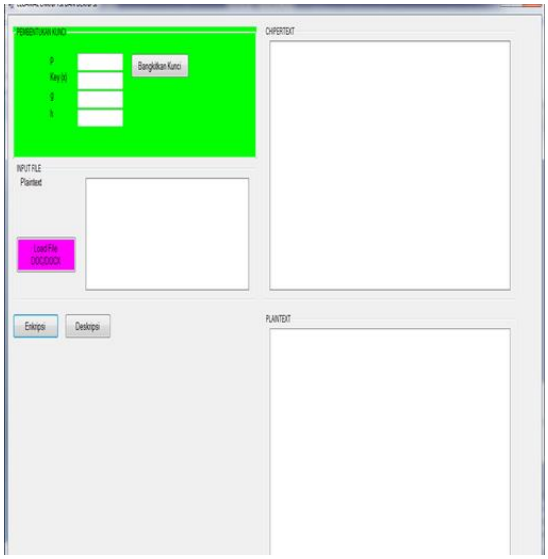
Setelah melalui proses pembuktian kebenaran hasil dari perhitungan dekripsi yang diubah menjadi teks kembali dengan menggunakan *ASCII*, maka hasil akhir dekripsi berupa hasil perubahan nilai decimal *ASCII* kedalam karakter yang berupa ABCDEF.

e-ISSN : 2722-4368

Gambar 1. Tampilan Halaman Utama Sistem

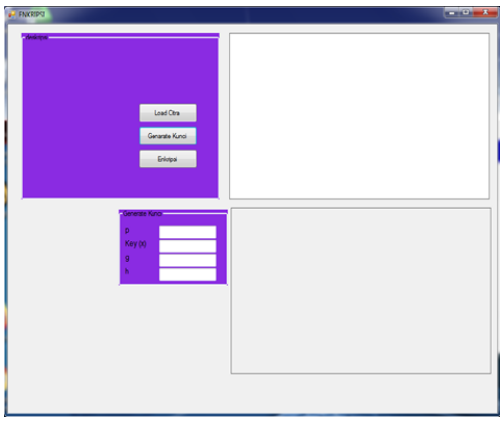


Gambar 2. Tampilan Halaman Proses Enkripsi Text ElGamal



Gambar 3. Tampilan Halaman Proses Enkripsi Docs ElGamal

e-ISSN : 2722-4368



Gambar 4. Tampilan Menu Proses Enkripsi Gambar ElGamal

KESIMPULAN

Setelah penulis melakukan analisis, perancangan, implementasi dan pengujian system pada penelitian yang berjudul Penerapan Enkripsi Dan Deskripsi Dengan Metode ElGamal Guna Meningkatkan Keamanan Data Text Dan Gambar, dapat ditarik kesimpulan sebagai berikut :

1. Dengan adanya aplikasi keamanan data text dan gambar maka data text Dan Gambar dapat diamankan dengan baik
2. Sistem yang dirancang ini dapat mengamankan data text dan gambar dengan baik dikarenakan menggunakan metode ElGamal
3. Sistem ini dapat mengamankan data text dan gambar dengan metode ElGamal

DAFTAR PUSTAKA

[1] Winda sari, analisa algoritma ElGamal dalam penyandian data sebagai keamanan database,jurnal informatika kaputama(jik), vol. 2 no. 1, januari 2018

[2] Nur fajrin maulana yusuf, pengiriman pesan dengan algoritma kriptografi ElGamal, jurnal matematika dan aplikasinya, vol 1 no 2, september 2019

[3] M. Taufiq tamam, penerapan algoritma kriptografi ElGamal untuk pengaman file citra, jurnal eeccis vol. Iv, no. 1, juni 2010

[4] Faqihuddin al-anshori, implementasi algoritma kriptografi kunci publik ElGamal untuk Proses enkripsi dan dekripsi guna pengamanan file data, jurnal informatika februari 2014.

[5] Ai Ilah Warnilah,Komparasi Algoritma Kriptografi ElGamal Dan Caesar Cipher Untuk Enkripsi Dan Dekripsi Pesan,IJCIT (Indonesian Journal on Computer and Information Technology) Vol.3, No.2, November 2018

[6] Aisyatul Karima, Ari Saputro, Pembangkitan Kunci Pada Algoritma Asimetris ElGamal untuk Meningkatkan Keamanan Databertipe.docx, Jurnal Ilmiah SISFOTENIKA Vol. 6, No. 2, Juli 2016

[7] Fajar Ibnu Wicaksana, Ir. Siswanto, Kiptografi Database Menggunakan Algoritma ElGamal Berbasis Web, SKANIKA Vol. 1 No. 1 Maret 2018

[8] Muhammad Rofiq, Perancangan dan Implementasi Algoritma Elgamal untuk Keamanan Data pada Video Streaming, Jurnal JITIKA, Vol. 6, No. 2. Agustus 2012