P-ISSN: 2548-9704
E-ISSN: 2686-0880

PEMANFAATAN USB FLASHDISK SEBAGAI KUNCI PADA KEAMANAN DATA DENGAN PENERAPAN ALGORITMA ELGAMAL

Rizka Putri Rahayu[1)], Achmad Fauzi[2)]

[2)]STMIK KAPUTAMA
Jl.Veteran No.4A-9A, Binjai, Sumatra Utara, Telp:(061)8828840, Fax: (061)8828845
Email: rizkaputrirahayu2@gmail.com[2)] fauzyrivai88@gmail.com[2)]

ABSTRACT

Cryptography is one of the sciences that studies mathematical techniques related to aspects of information security such as confidentiality. One cryptographic algorithm is the Elgamal algorithm to encrypt and decrypt messages that use a USB flash drive as a key. Flashdisk is widely used by students for data storage, therefore choosing flash as an encryption key is also very important and wants to be a reason to use flash as an encryption key and supporting device for data security. The use of flash as a medium for more secure data security. The problem that will be solved by using this system is security in the form of text files. in the process of encrypting text messages that can be read (plaintext) will be encrypted with an elgamal algorithm by using an elgamal algorithm key to produce a ciphertext. Implementation of the system uses visual basic.net software 2010. Then the decryption process is the process of returning a secret message (ciphertext) to the original message (plaintext). The USB device used to encrypt the plaintext must be the same as the USB device used to describe the ciphertext if the USB devices used are not the same, the decryption results are not the same as before encryption.

Keywords: Cryptography, Elgamal Algorithm, USB Flasdisk

ABSTRAK

Kriptografi merupakan salah satu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan. Salah satu algoritma kriptografi adalah Algoritma Elgamal pada enkripsi dan dekripsi pesan memanfaatkan usb flashdisk sebagai kunci. Flashdisk banyak digunakan oleh kalangan pelajar untuk penyimpanan data oleh sebab itu pemilihan flashdisk sebagai kunci enkripsi juga sangat penting dan ingin merupakan alasan penggunaan flashdisk sebagai kunci enkripsi dan perangkat pendukung dari sebuah keamanan data. Penggunaan flashdisk sebagai media agar keamanan data lebih terjamin, Masalah yang akan di selesaikan dengan menggunakan sistem ini adalah pengamanan berupa file teks. pada proses enkripsi pesan teks yang dapat di baca (plainteks) akan di enkripsi oleh algoritma elgamal dengan menggunakan kunci algoritma elgamal sehingga menghasilkan chiperteks. Implementasi sistem menggunakan perangkat lunak visual basic.net 2010. kemudian proses dekripsi adalah proses pengembalian pesan rahasia (chiperteks) menjadi pesan asli (plainteks). Perangkat usb digunakan untuk mengenkripsi plainteks harus sama dengan perangkat usb yang digunakaan untuk mendekripsikan chiperteks apabila perangkat usb yang digunakan tidak sama maka hasil dekripsi tidak sama seperti sebelum dienkripsi.

Kata kunci : Kriptografi, Algoritma *Elgamal, USB Flasdisk*

P-ISSN: 2548-9704
E-ISSN: 2686-0880

1. PENDAHULUAN

Dalam kriptografi terdapat beberapa algoritma yang dapat mengunci data dan masih banyak orang yang belum mengerti bagaimana mengunci ataupun mengamankan sebuah *file* sehingga tidak dapat dilihat oleh orang lain. Hal ini disebabkan rumitnya prosedur pengamanan komputer jika menggunakan fasilitas yang disediakan oleh masing-masing sistem operasi. Untuk itu, dibutuhkan sebuah aplikasi yang dapat dengan mudah dan cepat mengunci dan mengamankan komputer pengguna dengan menggunakan kata kunci yang diinputkan ke dalamnya.

Algoritma Elgamal menekankan pada permasalahan Algoritma diskrit. Dengan permasalahan tersebut maka cipherteks hasil enkripsi Elgamal akan sangat sulit di kriptanalis. Matematika diskrit yang dimaksud dalam kriptografi Elgamal adalah mencari sebuah bilangan pangkat (x), pada sebuah bilangan bulat (g). Dimana bilangan tersebut merupakan bilangan bulat lainnya (y) jika di mod dengan bilangan p (bilangan prima). kerumitannya terletak pada masalah diskrit karena melibatkan bilangan prima p sebagai variabel modulo dan x adalah bilangan yang dicari berupa bilangan pangkat (Winda, 2018).

Untuk memperkuat latar belakang permasalahan, penulis memasukkan jurnal yang berkaitan dengan pengamanan *file* yang diteliti oleh ***Adhytio Sasmita Chan dan Permanan Ginting Munthe, MBA dengan judul Perancangan "Aplikasi Pengamanan file Dengan Memanfaatkan USB Flashdisk Sebagai Kunci Menggunakan Algoritma Tripple Des"Dan "Algoritma Elgamal Dalam Pengamanan Pesan Rahasia" Danang Tri Massandy .*** Dalam penelitian tersebut menjelaskan agar dapat menghasilkan pengamanan komputer berbasis kata kunci yang memiliki tingkat kerahasiaan yang tinggi, haruslah dilakukan penyandian terhadap kata sandi tersebut baik untuk proses penguncian maupun proses pembukaan kunci pengamanan. Salah satu metode penyandian yang digunakan adalah Metode tripple Des.

Sekarang ini *Flashdisk* banyak digunakan oleh kalangan pelajar untuk penyimpanan data dan oleh sebab itu pemilihan *Flashdisk* sebagai kunci enkripsi juga sangat penting dan ini merupakan alasan utama kenapa penulis memilih menggunakan *Flashdisk* sebagai kunci enkripsinya oleh karena itu *Flashdisk* sangat penting sebagai perangkat pendukung dari pada sebuah keamanan data. *Flashdisk* digunakan sebagai kunci terhadap *file text* yang akan di enkripsi, penggunaan *Flashdisk* akan lebih aman dikarenakan setiap *Flashdisk* tidak ada memiliki serial yang sama, tanpa *Flashdisk* mustahil *file* tersebut dapat di enkripsi ataupun di dekripsi.

2. METODOLOGI PENELITIAN

2.1 Pengenalan Kriptografi

Kriptografi berasal dari bahasa yunani: " cryptos" yang artinya "*secret*" (rahasia) dan "graphein" yang artinya "*writing*" (tulisan). Jadi Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping message secure*). (Ariyus, 2006, h. 9) . Menurut Munir (2008, h.20) Kriptografi adalah merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Kriptografi adalah proses penggunaan berbagai teknik dan atau ilmu dan seni untuk menjaga keamanan pesan.

Menurut Kromodimoeljo (2010, h. 25) Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan

P-ISSN: 2548-9704
E-ISSN: 2686-0880

suatu algoritma dengan beberapa parameter.
Menurut Ariyus (2006, h. 9), kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasian, keutuhan data, dan otentikasi entitas.

2.2 Algoritma Elgamal

Algoritma ini pada umumnya digunakan untuk digital signature, namun kemudian dimodifikasi sehingga bisa digunakan untuk enkripsi dan Keamanan algoritma Elgamal terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah logaritma 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 algoritma ini adalah membutuhkan *resource* yang besar karena cipherteks yang dihasilkan dua kali panjang plainteks serta membutuhkan *procesor* yang mampu untuk melakukan komputasi yang besar untuk perhitungan logaritma perpangkatan besar. (Kromodimoeljo, 2010)

Konsep pada algoritma elgamal meliputi :

a) Ambil sebuah karakter dalam pesan yang akan dienkripsi dan transformasi karakter tersebut ke dalam kode ASCII sehingga diperoleh bilangan bulat m. Plainteks tersebut disusun menjadi blok-blok m1, m2, …, sedemikian hingga setiap blok merepresentasikan nilai di dalam rentang 0 (nol) sampai p-1.
b) Memilih bilangan acak k, yang dalam hal ini 0 < k < p-1, sedemikian hingga k relative prima dengan p-1.
c) Hitung nilai a dan b dengan persamaan berikut :

$$a = g^k \pmod p \quad \ldots\ldots\ldots\ldots (4)$$

$$b = y^k \, m \pmod p \quad \ldots\ldots\ldots (5)$$

d) Diperoleh cipherteks untuk karakter m tersebut dalam blok (a,b)
e) Melakukan proses di atas untuk seluruh karakter dalam pesan termasuk karakter spasi.

Dekripsi dari cipherteks ke plainteks menggunakan kunci rahasia a yang disimpan kerahasiaanya oleh penerima pesan. (Suci, 2020).
Teorema :
Diberikan (p,g, y) sebagai kunci public dan x sebagai kunci rahasia pada algoritma Elgamal. Jika diberikan cipherteks (a, b), maka

$$m = b/a^x \bmod p \quad \ldots\ldots\ldots (4)$$

dengan M adalah plainteks.
Di mana nilai

$$(ax)^{-1} = r^{-a} = rp^{-1-a} \bmod p. \quad \ldots (5)$$

Ambil sebuah blok cipherteks dari pesan yang telah dienkripsikan pengirim.
Dengan menggunakan *a* yang dirahasiakan oleh penerima, hitung nilai plainteks dengan menggunakan "persamaan (4)" dan "persamaan (5)". (Fauzi.2016)

Secara garis besar algoritma Elgamal mempunya langkah-langkah pembentukan kunci sebagai berikut :
Bilangan prima, p (bersifat public atau tidak rahasia)

1. Bilangan acak, g (dimana g < p dan bersifat public atau tidak rahasia)
2. Bilangan acak, x (dimana x < p dan bersifat *private* atau rahasia)
3. Bilangan acak, k (dimana k < p dan bersifat *private* atau rahasia)
4. m merupakan plainteks dan bersifat *private*/rahasia
5. a dan b merupakan pasangan cipherteks hasil enkripsi bersifat *private* atau tidak rahasia.

Proses Pembentukan kunci Algoritma Elgamal Proses pembentukan kunci merupakan proses penentuan suatu

P-ISSN: 2548-9704
E-ISSN: 2686-0880

bilangan yang kemudian akan digunakan sebagai kunci pada proses enkripsi dan dekripsi pesan. Kunci untuk enkripsi dibangkitkan dari nilai p, g, y sedangkan kunci untuk dekripsi terdiri dari nilai x, p. Masing-masing nilai mempunyai persyaratan yang harus dipenuhi.
Langkah-langkah dalam pembuatan kunci adalah sebagai berikut :

1. Pilih sembarang bilangan prima p, dengan syarat p > 211
2. Pilih bilangan acak g dengan syarat g < p.
3. Pilih bilangan acak x dengan syarat $1 \leq x \leq p - 2$.
4. Hitung $y = g^{\wedge x} \bmod p$.

Kunci publiknya adalah y, g, p sedangkan kunci *private* nya adalah x. nilai y, g, dan p tidak dirahasiakan sedangkan nilai x harus dirahasiakan karena merupakan kunci *private* untuk mendekripsi plainteks. (fauzi, 2018).

2.3 USB *Flashdisk*

USB *Flashdisk* merupakan sebuah *hardware* yang biasa digunakan untuk menyimpan *file-file* yang ada di komputer, sehingga *file* tersebut bisa dibawa kemana saja dan kapan saja bisa di modifikasi. Penggunaan *flashdisk* sebagai kunci sangat tepat dirasa karena hal ini seperti hardware dongle (USB Dongle) yang biasa digunakan sebagai *password* untuk masuk ke sistem seperti pada *software magic* dan *zahir accounting* yang menggunakan USB Dongle sebagai kunci akses.

Sebenarnya spesifikasi usb *flashdisk* tidak di batasi, dan bisa menggunakan kapasitas usb *flashdisk* yang berapa saja sehingga dalam proses proteksi atau proses penyandian dapat berjalan dengan konsistensi. *Flashdisk* tentunya seperti *hardware* lainnya mempunyai serial number yang unik dan tidak akan mungkin sama dikarenakan memiliki *register base assembly* yang berbeda walaupun memiliki IC yang sama, penggunaan serial number *flashdisk* tersebut lah yang diakses untuk dijadikan kunci sehingga hanya user yang memiliki *flashdisk* tersebut saja yang bisa melakukan proses enkripsi dan dekripsi.

2.4 Manajemen Kunci

Aspek manajemen kunci sangat penting dalam aplikasi kriptografi. Manajemen kunci yang tidak baik dapat berakibat fatal. Proses pembuatan kunci sangat penting dan sebaiknya proses ini benar acak. Sumber acak (entropi) dapat diambil dari proses fisika acak seperti proses radio-aktif. Sumber acak dapat juga diambil dari berbagai kejadian (*events*) yang muncul secara acak. Aplikasi kriptografi dapat menggunakan *random number generator* yang disediakan *operating system* untuk pembuatan kunci, akan tetapi sebaiknya ini dilakukan hanya jika *random number generator* yang disediakan cukup acak. **(**Kromodimoeljo, 2010).

3. HASIL DAN PEMBAHASAN

3.1 Analisa Hasil Perhitungan Algoritma El-Gamal

Pada proses enkripsi algoritma elgamal tersebut diasumsikan mempunyai panjang maksimal penentuan bilangan prima adalah P = 211, langkah selanjutnya melakukan analisis enkripsi pesan pada Algoritma Elgamal yang bertujuan untuk merubah pesan asli (plaintext) ke bentuk pesan rahasia (ciphertext). Adapun urutan proses pesan tersebut adalah :

1. Masukan teks yang akan dienkripsi *(Plaintext)*
   Plaintext = **“ R I Z K A P R O “**
2. Pesan akan di potong menjadi blok – blok karakter dan di konversikan ke dalam bilangan ASCII.

Tabel 1. Konversi Blok karakter ke dalam kode ASCII

P-ISSN: 2548-9704
E-ISSN: 2686-0880

I	Karakter	Planiteks Mi	Plainteksmi (ASCII)
1	**R**	M_1	**82**
2	**I**	M_2	**73**
3	**Z**	M_3	**90**
4	**K**	M_4	**75**
5	**A**	M_5	**65**
6	**P**	M_6	**80**
7	**R**	M_7	**82**
8	**O**	M_8	**79**

3. Langkah selanjutnya, Proses menentukan bilangan acak $P \in \{0,1, \dots \dots \dots .211\}$ kemudian nilai ASCII tersebut dimasukkan kedalam blok-blok nilai m secara berurutan, sehingga menjadi :

Mn	Nilai	Kunci
m1	**82**	**23**
m2	**73**	**13**
m3	**90**	**41**
m4	**75**	**105**
m5	**65**	**27**
m6	**80**	**90**
m7	**82**	**117**
m8	**79**	**53**

kemudian di hitung $y \equiv g^x \ mod \ p$ dan $m1 \equiv b1.a1^{p-1-x} \ mod \ p$
Misalkan Acak membangkitkan pasangan kunci dengan memilih bilangan:
p = 211
g = 13
x = 7
Kemudian p, g, x digunakan untuk menghitung y :
$y \equiv g^x \ mod \ p$
$y \equiv 13^7 \ mod \ 211$
$\boldsymbol{y \equiv 71}$
Hasil algoritma ini adalah :
kunci publik adalah triple (71, 13, 211)
kunci private adalah pasangan (7, 211)

dimana Enkripsi a adalah :

$\boldsymbol{a \equiv g^k \ mod \ p}$
$a1 \equiv 13^{23} \ mod \ 211$
$a1 \equiv \mathbf{11}$
$a2 \equiv 13^{13} \ mod \ 211$
$a2 \equiv \mathbf{193}$
$a3 \equiv 13^{41} \ mod \ 211$
$a3 \equiv \mathbf{184}$
$a4 \equiv 13^{105} \ mod \ 211$
$a4 \equiv \mathbf{1}$
$a5 \equiv 13^{27} \ mod \ 211$
$a5 \equiv \mathbf{203}$
$a6 \equiv 13^{90} \ mod \ 211$
$a6 \equiv \mathbf{199}$
$a7 \equiv 13^{17} \ mod \ 211$
$a7 \equiv \mathbf{96}$
$a8 \equiv 13^{53} \ mod \ 211$
$a8 \equiv \mathbf{151}$
dimana Enkripsi b adalah :
$\boldsymbol{b \equiv y^k \, m \ mod \ p}$
$b1 \equiv 71^{23} \ 82 \ mod \ 211$
$\boldsymbol{b1 \equiv 79}$
$b2 \equiv 71^{13} \ 73 \ mod \ 211$
$\boldsymbol{b2 \equiv 6}$
$b3 \equiv 71^{41} \ 90 \ mod \ 211$
$\boldsymbol{b3 \equiv 60}$
$b4 \equiv 71^{105} \ 75 \ mod \ 211$
$\boldsymbol{b4 \equiv 75}$
$b5 \equiv 71^{27} \ 65 \ mod \ 211$
$\boldsymbol{b5 \equiv 193}$
$b6 \equiv 71^{90} \ 80 \ mod \ 211$
$\boldsymbol{b6 \equiv 80}$
$b7 \equiv 71^{117} \ 82 \ mod \ 211$
$\boldsymbol{b7 \equiv 13}$
$b8 \equiv 71^{53} \ 79 \ mod \ 211$
$\boldsymbol{b8 \equiv 205}$

Setelah mendapatkan nilai enkripsi a dan b, hasil perhitungan tersebut disusun dengan pola selang seling:
a1, b1, a2, b2, a3, b3, a4, b4, a5, b5, a6, b6, a7, b7, a8, b8.
Sehingga membentuk cipherteks :
11, 79, 193, 6, 184, 60, 1, 75, 203, 193, 199, 80, 96, 13, 151, 205.

Di dalam bentuk karakter menjadi : **VT,t,┴,Ä,©,┬,SOH,U,╤,▒, Ä,A,Ç,ŭ, Ä.**
Proses Dekripsi Algoritma Elgamal

P-ISSN: 2548-9704
E-ISSN: 2686-0880

Cipherteks akan di potong menjadi blok – blok karakter dan di konversikan ke dalam bilangan ASCII.

Tabel 2. Konversi Blok Cipherteks ke dalam kode ASCII

I	Karakter	Planiteks Mi	Plainteksmi (ASCII)
1	VT	M_1	11
2	T	M_2	79
3	⊥	M_3	193
4	Ä	M_4	6
5	©	M_5	184
6	⊤	M_6	60
7	SOH	M_7	1
8	U	M_8	75
9	╥	M_9	203
10	▒	M_{10}	193
11	Ä	M_{11}	199
12	A	M_{12}	80
13	‘	M_{13}	96
14	Ç	M_{14}	13
15	Ù	M_{15}	151
16	Ä	M_{16}	205

mendekripsikan chiperteks dari B dengan melakukan perhitungan dengan rumus sebagai berikut :

$cn \equiv bi.ai^{p-1-x} \ mod\ 211$
$c1 \equiv 79.11^{211-1-7} \ mod\ 211$
$c1 \equiv 79.11^{203} \ mod\ 211$
$\boldsymbol{c1 \equiv 82}$
$c2 \equiv 6.193^{211-1-7} \ mod\ 211$
$c2 \equiv 6.193^{203} \ mod\ 211$
$\boldsymbol{c2 \equiv 73}$
$c3 \equiv 60.184^{211-1-7} \ mod\ 211$
$c3 \equiv 60.184^{203} \ mod\ 211$
$\boldsymbol{c3 \equiv 90}$
$c4 \equiv 75.1^{211-1-7} \ mod\ 211$
$c4 \equiv 75.1^{203} \ mod\ 211$
$\boldsymbol{c4 \equiv 75}$
$c5 \equiv 193.203^{211-1-7} \ mod\ 211$
$c5 \equiv 193.203^{203} \ mod\ 211$
$\boldsymbol{c5 \equiv 65}$
$c6 \equiv 80.199^{211-1-7} \ mod\ 211$
$c6 \equiv 80.199^{203} \ mod\ 211$
$\boldsymbol{c6 \equiv 80}$
$c7 \equiv 13.96^{211-1-7} \ mod\ 211$
$c7 \equiv 13.96^{203} \ mod\ 211$
$\boldsymbol{c7 \equiv 82}$
$c8 \equiv 205.151^{211-1-7} \ mod\ 211$
$c8 \equiv 205.151^{203} \ mod\ 211$
$\boldsymbol{c8 \equiv 79}$

Setelah mendapatkan nilai mn, masing-masing nilai m hasil dekripsi menjadi kode ASCII diubah kembali menjadi karakter. Dengan hasil sebagai berikut :

Tabel 3. Konversi plainteks ASCII ke karakter

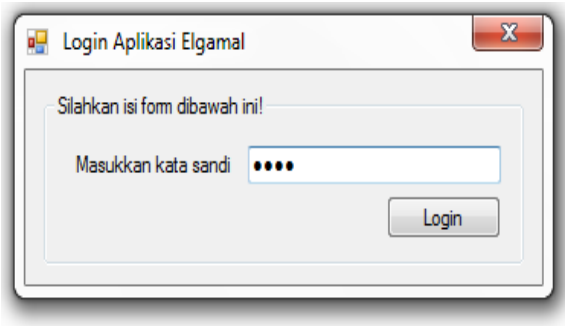
Plainteks Kode ASCII	Karakter
82	R
73	I
90	Z
75	K
65	A
80	P
82	R
79	O

3.2 PEMBAHASAN

Pada Penelitian ini sistem dibangun menggunakan Visual Basic.Net 2010, dimana implementasi pembahasan aplikasi yang dikembangkan dapat dilihat pada gambar di bawah ini.

1. Form Login

Form ini digunakan untuk melakukan proses login masuk ke sistem, caranya dengan memasukkan kata sandi seperti terlihat pada gambar dibawah ini :

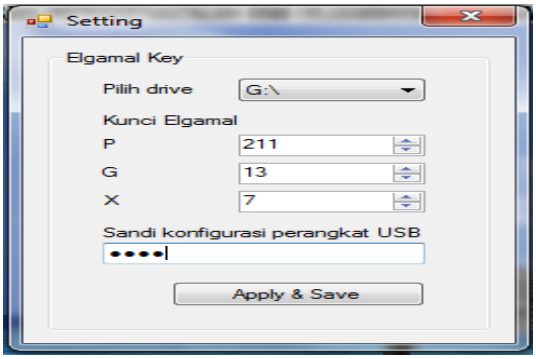


Gambar 1. Form Login

P-ISSN: 2548-9704
E-ISSN: 2686-0880

2. Fom Setting USB

Tampilan Form Setting USB dapat terlihat pada gambar di bawah ini :

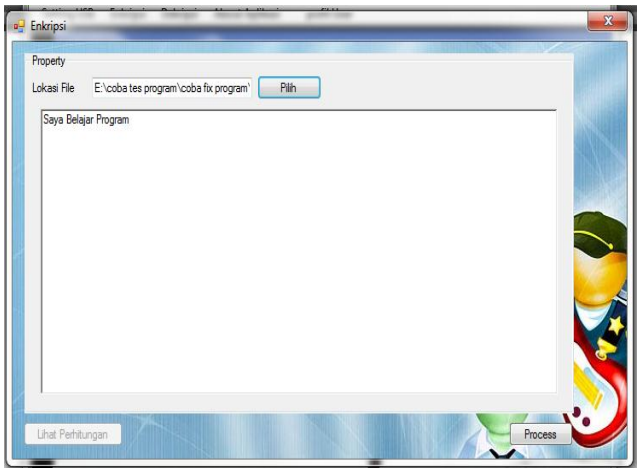


Gambar 2. Form Setiting USB

Form Setting USB digunakan untuk melakukan proses pengaturan USB dengan cara pilih drive dimana lokasi *flashdisk* kemudian memasukan kunci algoritma Elgamal dengan menginputan nilai P, G, X dan selanjutnya memasukkan sandi konfigurasi perangkat USB lalu pilih tombol apply dan save

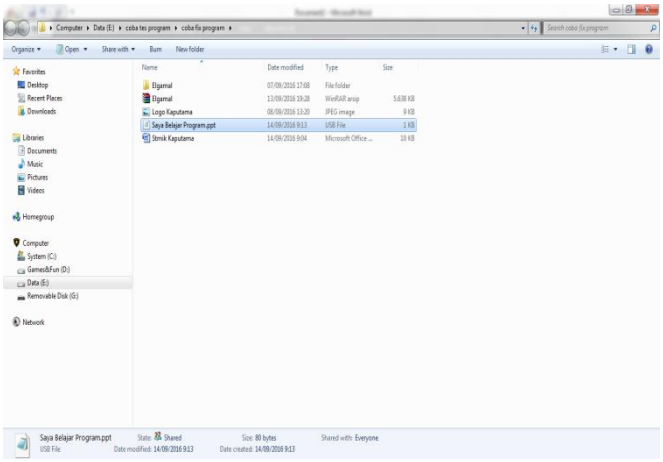
3. Form Enkripsi

Pada Form Enkripsi kita dapat memilih file text yang akan di enkripsikan seperti gambar di bawah berikut:



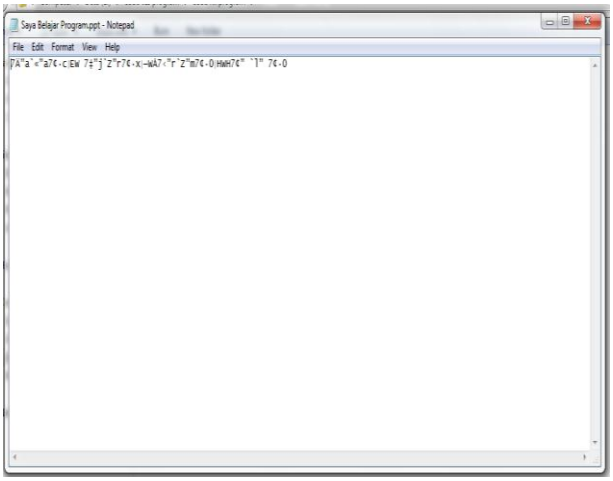
Gambar 3. Enkripsi File Teks

Berikut merupakan tampilan gambar untuk pemilihan file teks yang akan dienkripsi :



Gambar 4. Proses Pengambilan File

Setelah melakukan enkripsi plainteks hasilnya dapat dilihat pada gambar di bawah ini :



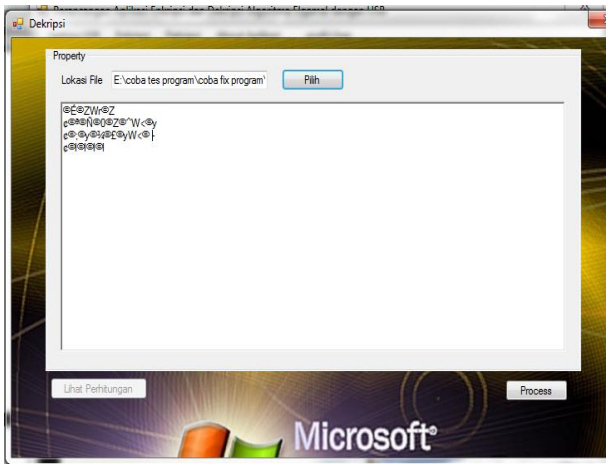
Gambar 5. Hasil Enkripsi

Gambar 5. Merupakan hasil enkipsi file teks sehingga isi pesan tidak dapat dibaca oleh pihak yang tidak berwenang.

4. Form Dekripsi

Berikut merupakan proses pengambilan chiperteks menjadi plainteks :

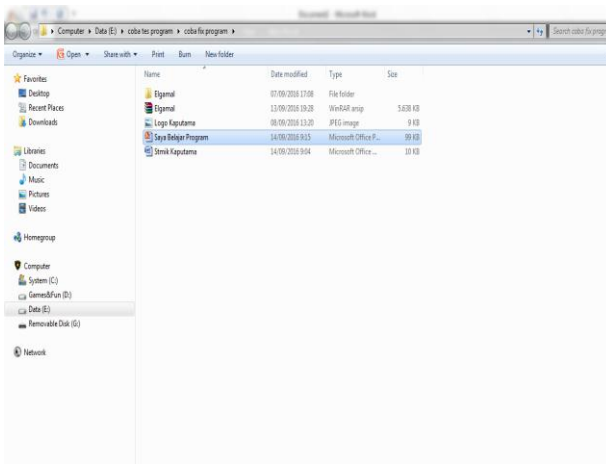
P-ISSN: 2548-9704
E-ISSN: 2686-0880



Gambar 6. Proses Dekripsi

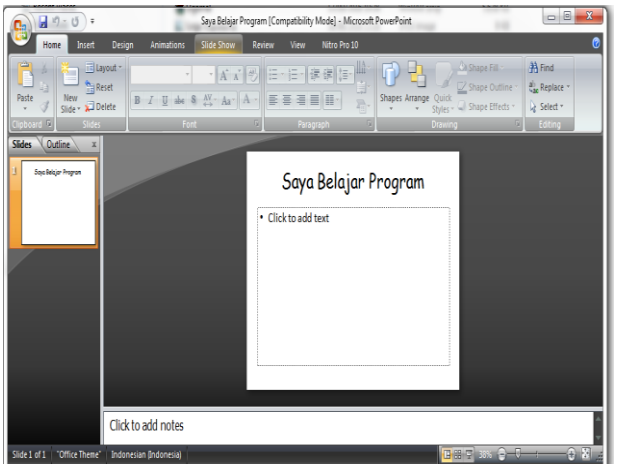
Pada Gambar 6. proses dekripsi dilakukan untuk mengembalikan pesan rahasia (chiperteks) menjadi pesan asli (Plainteks) dengan cara memilih file yang telah dienkripsi kemudian pilih tombol proses.

Berikut merupakan pengambilan file teks dari file yang terdapat di komputer :



Gambar 7. Proses Pemilihan File Teks

Setelah melakukan dekripsi pesan maka menghasilkan pesan asli (plainteks). yang terdapat pada gambar di bawah ini :



Gambar 8. Hasil Dekripsi

Gambar 8. Hasil Dekripsi pesan rahasia (Chiperteks) pesan asli (Plainteks).

4. KESIMPULAN

Berdasarkan Pembahasan diatas dan setelah dilakukan penelitian dan pengujian, maka didapat kesimpulan :

1. Perangkat usb yang digunakan untuk mengenkripsi plainteks harus sama dengan perangkat usb yang digunakan untuk mendekripsikan cipherteks. Apabila perangkat usb yang digunakan untuk menegekripsi tidak sama dengan perangkat usb yang digunakan untuk mendekripsi, maka hasil dari dekripsi tidak akan sama dengan plainteks semula seperti sebelum di enkripsi.
2. Program aplikasi kriptografi ini dapat mengamankan sebuah data rahasia sehingga data lebih terjamin keamanannya.
3. Proses enkripsi pesan akan menghasilkan sebuah pesan rahasia (chiperteks), kemudian proses dekripsi untuk mengembalikan pesan rahasia menjadi pesan asli (plainteks).

5. SARAN

Berikut ini adalah saran yang dapat digunakan untuk tahap pengembangan sistem ini :

1. Apabila dalam proses penggunaan sistem aplikasi ini flashdisk di

P-ISSN: 2548-9704
E-ISSN: 2686-0880

cabut dari perangkat maka sistem akan terhenti.

2. Sistem ini menggunakan Algoritma Elgamal, dengan kunci yang digunakan adalah USB Flashdisk, sehingga untuk pengembangan selanjutnya dapat mengenkripsikan dan dekripsi file teks dengan menggunakan USB Flashdisk sebagai kunci.
3. File yang dapat di enkripsikan dan di dekripsi dalam sistem file dengan ekstensi *txt, *doc, *ppt, *xls. agar bisa menggunakan file dengan jenis ekstensi lainnya.
4. Aplikasi ini diharapkan dapat dikembangkan dengan metode-metode yang lainnya sebagai perbandingan dan menjadi sistem yang lebih mendekati kepada keperawatan serta solusi yang lebih baik

DAFTAR PUSTAKA

[1]. Fauzi, Achmad dan Maulita, Yani. (2016). Analisis Hybrid Crytosystem Algoritma Elgamal dan Algoritma Triple DES.

[2]. Adhityo Samitha Chan dan Permana Ginting Munthe. 2014. Perancangan Aplikasi Pengamanan File Dengan Memanfaatkan USB Flashdisk Sebagai Kunci Menggunakan Algoritma Triple DES. Jurnal ISSN : 2301-9425.

[3]. Rifki Sadikin. 2012. *Kriptografi Untuk Keamanan Jaringan.* Penerbit Andi. Yogyakarta

[4]. Sentot Kromodimoeljo.2009.Teori Dan Aplikasi Kriptografi. Penerbit SPK IT Consulting.

[5]. Sari, Winda, Maulita, Yani & Fauzi, Achmad. (2018). Analisa Algoritma Elgamal Dalam Penyandian Data Sebagai Keamanan Database.

[6]. Doni Ariyus. (2006). *Kriptografi Keamanan Data Dan Komunikas*i.Penerbit Graha Ilmu. Yogyakarta

[7]. Fauzi, Achmad, dan Maulita, Yani. (2018). Perancangan Aplikasi Keamanan Pesan Menggunakan Algoritma Elgamal Dengan Memanfaatkan Algoritma One Time Pad Sebagai Pembangkit Kunci. JTIK (Jurnal Teknik Informatika Kaputama), 1(1), 1-9.

[8]. Pardede, A. M. H. (2018). Aplikasi pengamanan file gambar menggunakan algoritma elgamal. *Journal Information System Development (ISD)*, *3*(2).

[9]. Ramandani, Suci. (2020). Hybird Cryptosystem Algoritma Hill Cipher Dan Algoritma Elgamal Pada Keamanan Citra, Jurnal Methomika, Volume. 4. Nomor. 1 April 2020.