Peningkatan Proteksi dengan Kombinasi El Gamal dan Playfair Cipher

Janice Laksana and 13510035[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13510035@std.stei.itb.ac.id

***Abstract*—Kriptografi adalah seni dan ilmu mengamankan pesan. Algoritma Playfair Cipher dan algoritma ElGamal adalah contoh algoritma kriptografi. Algoritma Playfair Cipher ditemukan oleh seorang pioneer telegraf, Charles Whetstone, dan dipopularkan oleh Lyon Playfair. Algoritma Algoritma Playfair Cipher ini merupakan algoritma klasik. Algoritma ElGamal ditemukan oleh Taher pada tahun 1985. Algoritma ini merupakan algoritma modern. Kombinasi dari algoritma Playfair Cipher dan algoritma ElGamal akan meningkatkan tingkat keamanan pesan sehingga pesan yang telah dienkripsi pun akan menjadi lebih sulit untuk dikriptanalisis. Dengan mengkombinasikan algoritma klasik dan algoritma modern ini, algoritma yang merupakan hasil kombinasi dapat dipakai pada masa mendatang.**

***Kata Kunci*—Algoritma Playfair Cipher, Algoritma ElGamal, Kombinasi Algoritma, Peningkatan Keamanan**

I. PENDAHULUAN

Kirptografi adalah seni dan ilmu dalam mengamankan pesan. Untuk menjaga kerahasiaan sebuah pesan, kriptografi mentransformasikan data atau pesan yang biasa dikenal sebagai plainteks ke dalam bentuk data sandi atau yang biasa dikenal sebagai cipherteks yang tidak dapat dikenali. Pengirim akan mengirimkan cipherteks ini kepada penerima. Setelah cipherteks sampai, cipherteks ini akan ditransformasikan lagi ke dalam bentuk plainteks sehingga data atau pesan yang dikirimkan dapat dibaca oleh penerima. Transformasi pesan ini biasanya menggunakan sebuah kunci yang telah disepakati oleh pengirim dan penerima sebelumnya.

Terdapat banyak sekali algoritma kriptografi, beberapa di antaranya adalah algoritma Playfair Cipher dan algoritma ElGamal. Algoritma Playfair Cipher merupakan algoritma klasik yang ditemukan oleh seorang pioneer telegraf yang bernama Charles Wheatstone dan dipopularkan oleh Lyon Playfair. Algoritma Playfair Cipher termasuk ke dalam polygram cipher di mana proses enkripsi dengan menggunakan algoritma ini akan dilakukan pada pasangan-pasangan huruf pesan. Keamanan pada algoritma Playfair Cipher ini adalah dengan mengenkripsikan pasangan-pasangan huruf, hasil enkripsi akan sulit untuk dianalisis dengan menggunakan perhitungan frekuensi kemunculan huruf.

Algoritma ElGamal adalah salah satu algoritma modern yang ditemukan oleh Taher ElGamal pada tahun 1985. Proses enkripsi pesan dengan menggunakan algoritma ini menggunakan kunci asimetris sebagai kunci publiknya di mana kunci publik ini berbasiskan pertukaran kunci Diffie-Hellman. Keamanan pada algoritma ElGamal ini terletak pada perhitungan logaritma diskrit yang sulit.

Makalah ini akan membahas mengenai kombinasi dari kedua algoritma di atas yaitu algoritma Playfair Cipher dan algoritma ElGamal menjadi algoritma PlayGamal (Playfair dan ElGamal). Kombinasi dari kedua algoritma ini bertujuan untuk meningkatkan keamanan suatu pesan. Algoritma PlayGamal ini menggabungkan dua algoritma dengan kelebihannya masing-masing di dalam tingkat keamanannya. Dengan menggunakan algoritma PlayGamal untuk mengenkripsi suatu pesan, hasil dari enkripsi akan semakin sulit untuk dikriptanalisis atau dipecahkan oleh kriptanalis.

II. DASAR TEORI

A. Playfair Cipher

Playfair Cipher merupakan salah satu contoh algoritma klasik yang ditemukan oleh Charles Wheatstone, salah seorang pioneer telegraf. Kemudian algoritma ini dipopularkan oleh Lyon Playfair pada tahun 1854. Algoritma Playfair Cipher termasuk ke dalam polygram cipher.

Proses enkripsi dengan algoritma Playfair Cipher, dilakukan dengan mengenkripsi pasangan-pasangan huruf bukan huruf-huruf tunggal. Tujuan proses enkripsi yang dilakukan perpasangan huruf ini adalah membuat analisis yang menggunakan perhitungan frekuensi kemunculan huruf menjadi sulit. Perhitungan tersebut menjadi sulit karena frekuensi kemunculan huruf-huruf dari cipherteks yang dihasilkan oleh proses enkripsi menggunakan algoritma ini menjadi datar.

Kunci yang digunakan dalam proses enkripsi, disusun di dalam sebuah bujur sangkar yang memiliki ukuran 5x5. Di dalam bujur sangkar ini akan terdapat semua alfabet namun tanpa huruf J.

Untuk melakukan proses enkripsi dengan algoritma Playfair Cipher, dilakukan dengan terlebih dahulu mengisi bujur sangkar kunci. Proses pengisian bujur sangkar kunci ini dilakukan pertama-tama dengan kesepakatan pengirim

pesan dan penerima pesan akan kata kunci yang akan digunakan. Kata kunci ini akan dituliskan pada bujur sangkar. Setelah itu sisa dari elemen-elemen bujur sangkar kunci yang belum diisi, akan diisi dengan alfabet A-Z tanpa huruf J yang belum ada pada bujur sangkar kunci. Sebagai contoh, misalkan kata kunci yang disetujui oleh pengirim dan penerima pesan adalah CHARLES, maka akan dibentuk bujur sangkar kunci seperti berikut :

C	H	A	R	L
E	S	B	D	F
G	I	K	M	N
O	P	Q	T	U
V	W	X	Y	Z

Setelah bujur sangkar kunci diisi, proses enkripsi dilanjutkan dengan proses pengaturan pesan yang akan dienkripsi. Proses pengaturan pesan ini adalah sebagai berikut :

1. Huruf J yang terdapat pada pesan diubah dengan huruf I.
2. Kemudian, tulis pesan dalam pasangan-pasangan huruf atau bigram.
3. Bila ada pasangan huruf yang memiliki huruf yang sama, sisipkan huruf Z di tengahnya.
4. Bila jumlah huruf pada pesan ganjil, tambahkan pada akhir pesan huruf Z.

Contoh proses pengaturan pesan :

PESAN :
MEET ME AT HAMMERSMITH BRIDGE TONIGHT

HASIL PENGATURAN :
ME ET ME AT HA MZ ME RS MI TH BR ID GE TO NI GH TZ

Setelah proses pengaturan pesan dilakukan, akan dilakukan algoritma enkripsi pada pesan yaitu dengan ketentuan-ketentuan sebagai berikut :

1. Dua huruf yang terdapat pada baris yang sama di dalam bujur sangkar kunci, akan dienkripsi menjadi huruf yang berada di kanannya.
2. Dua huruf yang terdapat pada kolom yang sama di dalam bujur sangkar kunci, akan dienkripsi menjadi huruf yang berada di bawahnya.
3. Jika dua huruf tidak berada pada baris maupun kolom yang sama di dalam bujur sangkar kunci, maka huruf pertama akan dienkripsi menjadi huruf yang terletak pada perpotongan antara baris huruf pertama dengan kolom huruf kedua. Sedangkan huruf kedua akan dienkripsi menjadi huruf yang terletak pada titik sudut keempat dari persegi panjang yang dibentuk dari tiga huruf yang telah digunakan.

Contoh :

BUJUR SANGKAR KUNCI :

C	H	A	R	L
E	S	B	D	F
G	I	K	M	N
O	P	Q	T	U
V	W	X	Y	Z

PESAN YANG TELAH DIATUR :
ME ET ME AT HA MZ ME RS MI TH BR ID GE TO NI GH TZ

HASIL ENKRIPSI :
GD DO GD RQ AR NY GD HD NK PR DA MS OG UP GK IC UY

B. ElGamal

Algoritma ElGamal merupakan salah satu algoritma modern yang ditemukan oleh Taher ElGamal pada tahun 1985. Algotma Enkripsi ElGamal merupakan algoritma enkripsi yang menggunakan kunci asimetris untuk kunci publiknya di mana kunci publik ini berbasis pertukaran kunci Diffie-Hellman.

Keamanan pada algoritma ElGamal terletak pada perhitungan logaritma diskrit yang sulit. Properti-properti dari algoritma ElGamal ini adalah :

1. p merupakan bilangan prima dan bersifat tidak rahasia.
2. g merupakan bilangan acak di mana g < p.
3. x adalah kunci privat yang merupakan bilangan acak di mana x < p.
4. y adalah kunci publik yang diperoleh dari hasil perhitungan g^x mod p dan bersifat tidak rahasia.
5. m adalah pesan yang akan dienkripsi.
6. a dan b merupakan cipherteks yang bersifat tidak rahasia.

Algoritma pembangkitan kunci ElGamal dilakukan sebagai berikut :

1. Memilih bilangan prima p secara sembarang.
2. Memilih dua bilangan acak yaitu bilangan g dan x yang memenuhi syarat g < p dan $1 \leq x \leq p-2$.
3. Menghitung y dengan rumus :

$$y = g^x \bmod p$$

Hasil dari pembangkitan kunci ElGamal ini adalah :

- Kunci publik : triple <y, g, p>
- Kunci privat : pasangan <x, p>

Algoritma enkripsi dilakukan sebagai berikut :

1. Menyusun pesan menjadi blok-blok m_1, m_2, dst di mana nilai setiap blok berada pada selang [0, p-1].
2. Memilih bilangan acak k yang memenuhi syarat $1 \leq k \leq p-2$.
3. Blok-blok yang telah disusun, masing-masing dienkripsi dengan menggunakan rumus :

$$a = g^x \bmod p$$
$$b = y^k m \bmod p$$

Pasangan dari a dan b merupakan cipherteks untuk blok pesan m. Dengan demikian, dapat diketahui apabila ukuran cipherteks yang dihasilkan dari proses ini akan menjadi dua kali lipat ukuran pesannya.

III. IMPLEMENTASI DAN ANALISIS

Ide dari implementasi program PlayGamal (Playfair Cipher and ElGamal) ini adalah dengan mengkombinasikan algoritma El Gamal dan algoritma Playfair Cipher. Proses enkripsi akan dilakukan dengan melakukan proses enkripsi dengan menggunakan algoritma Playfair Cipher terlebih dahulu, di mana pada proses enkripsi ini akan terdapat tahap di mana pengisian bujur sangkar kunci, pengaturan pesan yang akan dienkripsi, dan proses terakhir dari algoritma Playfair Cipher ini adalah proses enkripsi pesan yang telah terlebih dahulu diatur.

Cipherteks yang dihasilkan dari algoritma Playfair Cipher ini, akan dienkripsi kembali dengan menggunakan algoritma El Gamal sehingga cipherteks yang dihasilkan dari kombinasi kedua algoritma ini akan memiliki sifat yang sama dengan algoritma El Gamal, yakni ukuran dari cipherteks akan menjadi dua kali panjang dari pesan yang dienkripsi. Cipherteks ini merupakan heksadesimal.

Proses dekripsi cipherteks akan dilakukan dengan mendekripsi cipherteks terlebih dahulu dengan menggunakan algoritma ElGamal dan kemudian hasil dekripsi dari algoritma ElGamal ini akan didekripsi kembali dengan menggunakan algoritma Playfair Cipher. Dalam implementasinya, program PlayGamal ini memiliki beberapa fungsi-fungsi utama yaitu :

- Fungsi untuk mengisikan bujur sangkar kunci Playfair Cipher.
- Fungsi untuk mengenkripsi menggunakan algoritma Playfair Cipher (termasuk di dalamnya fungsi untuk mengatur pesan yang akan dienkripsi)
- Fungsi untuk mendekripsi dengan menggunakan algoritma Playfair Cipher.
- Fungsi untuk meng-*generate* kunci untuk algoritma ElGamal.
- Fungsi untuk mengenkripsi dengan menggunakan algoritma ElGamal.
- Fungsi untuk mendekripsi dengan menggunakan algoritma ElGamal.

Mengisi Bujur Sangkar Kunci Playfair Cipher

Mengisikan bujur sangkar kunci yang berukuran 5x5 dengan kunci yang merupakan masukan input dan huruf alfabet lain yang belum terkandung dalam kunci. Sebelum kunci dimasukkan, kunci terlebih dahulu diperiksa agar huruf-huruf yang terkandung di dalam kunci masukkan user tidak ada huruf yang berulang.

Mengenkripsi dengan Algoritma Playfair Cipher

Sebelum melakukan proses enkripsi dengan menggunakan algoritma Playfair Cipher, terlebih dahulu akan dilakukan pengaturan pesan yang akan dienkripsi. Pengaturan pesan ini berupa pembagian pesan ke dalam blok-blok bigram/pasangan huruf. Dengan menggunakan beberapa ketentuan, pembagian pesan ini tidak akan menghasilkan pasangan huruf di mana pasangan huruf ini terdiri dari dua huruf yang sama.

Proses enkripsi akan dilakukan dengan menggunakan bujur sangkar kunci dan akan menghasilkan sebuah cipherteks di mana sebelumnya spasi, yang tadinya digunakan untuk menandai bigram, dihapus terlebih dahulu.

Mendekripsi dengan Algoritma Playfair Cipher

Proses dekripsi dilakukan dengan menggunakan bujur sangkar kunci. Pada proses dekripsi ini, akan dihasilkan pesan yang mungkin tidak persis sama dengan aslinya (karena penyisipan huruf Z dan penggantian huruf I menjadi J yang dapat membuat beberapa kemungkinan hasil dekripsi). Sehingga untuk membuat proses dekripsi menjadi sempurna, dibutuhkan juga proses manual yang dilakukan oleh manusia yaitu misalkan apabila terdapat huruf Z di belakang hasil dekripsi, apakah dengan menghilangkan huruf Z akan diperoleh sebuah kalimat yang bermakna atau apakah dengan tidak menghilangkan huruf Z tersebut kalimat sudah bermakna.

Menggenerate Kunci

Menghasilkan kunci publik dan kunci privat secara random. Di mana kunci publik adalah pasangan <y, g, p> dan kunci privat adalah pasangan <x, p>.

Mengenkripsi dengan Algoritma ElGamal

Proses enkripsi dengan algoritma ElGamal dilakukan dengan mengikuti ketentuan-ketentuan dan rumus-rumus yang diberikan. Proses enkripsi ini akan menghasilkan hasil enkripsi dalam bentuk heksadesimal yang memiliki panjang dua kali dari panjang awal.

Mendekripsi dengan Algoritma ElGamal

Proses dekripsi dengan algoritma ElGamal dilakukan dengan mengikuti ketentuan-ketentuan serta rumus-rumus yang diberikan.

Interface Program Elgamal

Uji coba program ini adalah sebagai berikut :
Isi input file teks :

I dont wanna be someone who walks away so easily
Im here to stay and make the difference that I can make
Our differences they do a lot to teach us how to use
The tools and gifts we got yeah we got a lot at stake
And in the end youre still my friend at least we did intend
For us to work we didnt break we didnt burn
We had to learn how to bend without the world caving in
I had to learn what Ive got and what Im not and who I am

Kunci :

p : 6173 x : 1500
g : 2 y : 5601
k : 10
Kunci Playfair : charles

Hasil :

1. Proses enkripsi dengan algoritma PlayFair Cipher :

MSUGPYLKKLDSEPGDUGSVCPXHANBHXHWDVGH
BNHWMIRDCDOPEQRXRMFKRGBPRSFNSESCDGLD
OARPMHRGNBQGVTLSMNLESCDGLSBPRDVETRCP
UUPODRHLPISPVUPPFDOCSUPUCBHMFIKDUIHGOP
UVDRAVSOVQRCUQRPDQRGBLKSMMUCSFGMRPO
CDDPNHRNZDHMFGBRURBCDPVSSMSMMUFGFET
CPFUPVPAMVSSMFMQDCDBQVSSMFMQDTLIZSCR
BUPCFRLILPVUPDSMFHPPRPOUYPRSVTCRFHRWG
GIKGPSRBUPCFRLIZARPMCGOVQRMFHSRQKNGU
QRMFHSPGRK

Durasi : 0.0066221 sekon

2. Proses enkripsi dengan algoritma ElGamal :

0400034304000C0004000D6304001183040011230400
136304000C000400148304000C430400112304001123
04000C4304000C0004000CA304000DC304000C0004
0013030400118304001 0C304000DC30400118304001
12304000DC304000C000400148304000EE304001183
04000C000400148304000C4304001063040010030400
130304000C0004000C430400148304000C4304001543
04000C0004001303040011830400 0C0004000DC3040
00C430400130304000F4304001063040015430400 0C0
004000343040010C304000C0004000EE304000DC304
0012A304000DC304000C000400136304001183040 00
C000400130304001363040 0C4304000154304000C000
4000C430400112304000D6304000C00040010C30400
0C430400100304000DC304000C000400136304000EE
304000DC304000C0004000D6304000F4304000E2304
000E2304000DC3040012A304000DC3040011230400
0D0304000DC304000C000400136304000EE304000C
430400136304000C000400034304000C0004000D030
4000C430400112304000C00040010C304000C430400
100304000DC304000C000400058304001 3C3040012A
304000C0004000D6304000F4304000E2304000E2304
000DC3040012A304000DC3040011230400 0D030400
0DC304001303040 00C000400136304000EE304000D
C304001543040 00C0004000D6304001183040 00C000
4000C4304000C000400106304001183040013630400
C000400136304001183040 00C000400136304000
C000400148304001183040012A304001003
04000C000400148304000DC304000C0004000D63040
00F4304000D6304001123040013630400 0C0004000C
A3040012A304000DC304000C430400100304000C00
0400148304000DC304000C0004000D6304000F43040
00D6304001123040013630400 0C0004000CA3040013
C3040012A304001123040 00C000400088304000DC30
4000C0004000EE304000C4304000D6304000C000400
136304001183040 00C000400106304000DC304000C4
3040012A304001123040 00C0004000EE30400118304
00148304000C000400136304001183040 00C0004000C
A304000DC304001123040 00D6304000C00040014830
4000F4304001363040 00EE304001183040013C304001
36304000C000400136304000EE304000DC304000C00
0400148304001183040012A304001063040 00D630400
0C0004000D0304000C4304001423040 00F430400112
304000E8304000C0004000F4304001123040 00C00040
0034304000C0004000EE304000C4304000D6304000C
000400136304001183040 00C000400106304000DC30
4000C43040012A304001123040 00C00040014830400
0EE304000C4304001363040 00C0004003430400142
304000DC304000C0004000E8304001183040013630
000C0004000C4304001123040 00D6304000C0004001
48304000EE304000C4304001363040 00C0004000343
040010C304000C000400112304001183040013630400
0C0004000C4304001123040 00D6304000C000400148
304000EE304001183040 00C000400034304000C0004
000C43040010C3

Durasi : 0.0516879 sekon

3. Proses enkripsi dengan algoritma PlayGamal :

040004C304000703040007C304000283040005E30400
094304000463040004030400040304000463040001 63
04000703040001C3040005E30400028304000163040 0
07C3040002830400070304000823040001030400 05E3
040008E3040002E3040000430400052304000 0A30400
02E3040008E3040002E3040008830400016304000823
04000283040002E3040000A304000523040002E30400
0883040004C304000343040006A30400016304000103
040001630400058304000 5E3040001C3040006430400
06A3040008E3040006A3040004C3040002230400040
3040006A304000283040000A3040005E3040006A304
000703040002230400052304000703040001C3040007
030400010304000163040002830400046304000163 04
000583040000430400 06A3040005E3040004C3040002
E3040006A30400028304000523040000A3040006430
400028304000823040007630400046304000703040 00
4C3040005230400046304000 1C304000703040001030
400016304000283040004630400070304000 0A304000
5E3040006A3040001630400082304000 1C3040007630
40006A304000103040005E3040007C3040007C30400
05E3040005830400016304000 6A3040002E304000463
040005E3040003430400070304000 5E3040008230400
07C3040005E3040005E3040002230400016304000583
040001030400070304000 7C3040005E3040007C30400
0103040000A3040002E3040004C3040002230400034 3
040004030400016304000 7C304000343040002E30400
028304000583040005E3040007C30400082304000163
040006A3040000430400082304000703040005830400
082304000643040006A304000103040007C304000643
040006A3040005E3040001630400064304000 6A3040
00283040000A3040004630400040304000703040004C
3040004C3040007C3040001030400070304000223040
00283040004C3040006A3040005E3040005830400010
3040001630400016304000 5E304000523040002E3040
006A304000523040009A304000163040002E3040004
C3040002230400028304000 0A3040006A3040007C30
40006A3040000A3040001030400016304000 5E30400
082304000703040007030400 04C304000703040004C3
040004C3040007C3040002230400028304000223040 0
01C3040007630400010304000 5E304000223040007C3
040005E304000823040005E3040000430400 04C30400
082304000703040007030400 04C304000223040004C3
040006430400016304000103040001630400 0A30400
064304000823040007030400070304000 4C304000223
040004C3040006430400016304000763040004630400
0343040009A3040007030400010304000 6A3040000A
3040007C3040005E3040001030400022304000 6A3040
004630400034304000463040005E304000823040007C
3040005E3040001630400070304000 4C304000223040
002E3040005E3040005E3040006A3040005E3040005
83040007C304000943040005E3040006A30400070304
000823040007630400010304000 6A304000223040002
E3040006A3040008830400028304000 2830400034304
000403040002830400 5E304000703040006A3040000
A3040007C3040005E3040001030400022304000 6A30

400046304000343040009A304000043040006A304000
5E3040004C3040001030400028304000583040008230
4000643040006A3040004C304000223040002E304000
703040006A3040006430400040304000523040002830
40007C304000643040006A3040004C3040002230400
02E304000703040005E304000283040006A304000403

Durasi : 0.0364823 sekon

Screenshot Uji Coba :

4. Proses Dekripsi dengan Playfair Cipher
   Dengan input file ini, menghasilkan plainteks yang memiliki isi yang sama (tanpa manual manusia), namun format yang berbeda (tidak ada spasi). Durasi proses dekripsi adalah 0.0071335 sekon.

5. Proses Dekripsi dengan ElGamal
   Menghasilkan plaintext yang sama persis dengan isi teks pada awal mula dengan durasi 0.0072817 sekon.

6. Proses Dekripsi dengan PlayGamal
   Dengan input file ini, menghasilkan plainteks yang memiliki isi yang sama (tanpa manual manusia), namun format yang berbeda (tidak ada spasi). Durasi proses dekripsi adalah 0.0083832 sekon.

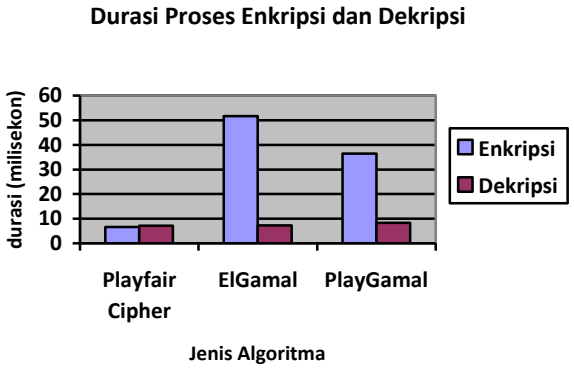
   Screenshot Uji Coba :

IV. KESIMPULAN

Mengkombinasikan algoritma ElGamal dengan algoritma Playfair Cipher yang merupakan kombinasi dari algoritma klasik dan algoritma modern, dapat meningkatkan keamanan pesan. Algoritma ElGamal memiliki keamanan yang terletak pada perhitungan logaritma diskrit yang sulit. Sedangkan algoritma Playfair Cipher sendiri memiliki keamanan yang terletak pada bujur sangkar kunci dan juga pada cara enkripsi yang menggunakan pasangan-pasangan huruf sehingga menyulitkan analisis dengan menggunakan perhitungan frekuensi kemunculan huruf. Dengan menggabungkan keduanya, cipherteks yang dihasilkan dari algoritma PlayGamal (Playfair and Elgamal) ini membuat kriptanalis sulit untuk memecahkan pesan yang terkandung di dalam cipherteks.

Pada uji coba, proses enkripsi yang dilakukan dengan menggunakan algoritma Playfair Cipher memiliki durasi 0.0066221 sekon. Proses enkripsi yang dilakukan dengan menggunakan algoritma ElGamal memiliki durasi 0.0516879 sekon. Sedangkan proses enkripsi yang dilakukan dengan menggunakan algoritma PlayGamal memiliki durasi 0.0364823 sekon.

Proses dekripsi yang dilakukan dengan algoritma Playfair Cipher menghasilkan hasil dekripsi dengan isi yang sama dengan file yang asli namun format yang berbeda (tidak ada spasi) dengan durasi 0.0071335 sekon. Sedangkan proses dekripsi dengan menggunakan algoritma ElGamal memiliki hasil yang memiliki isi yang dan format yang sama dengan file asli dengan durasi 0.0072817 sekon. Pada proses dekripsi dengan menggunakan algoritma PlayGamal dihasilkan hasil yang memilki isi yang sama dengan file asli namun format yang berbeda (tidak ada spasi) dan memiliki durasi 0.0083832 sekon.



REFERENSI

[1] http://www.simonsingh.net/The_Black_Chamber/playfair_cipher.html.. Tanggal Akses : 18 May 2013 jam 22.30.

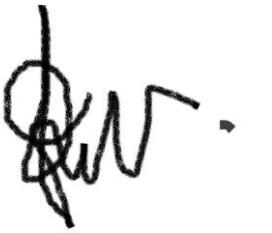
[2] http://www.princeton.edu/~achaney/tmve/wiki100k/docs/ElGamal_encryption.html. Tanggal Akses : 18 May 2013 jam 23.00.

[3] http://www.sarjanaku.com/2012/11/pengertian-kriptografi-definisi.html. Tanggal Akses : 19 May 2013 jam 18.00.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 May 2013



Janice Laksana
13510035