Jurnal Sistem Informasi ISSN P : 2598-599X; E: 2599-0330

ANALISIS KINERJA KOMBINASI ALGORITMA *AFFINE CHIPER*, *HILL CHIPER* DAN ALGORITMA EL GAMAL DALAMPENGAMANAN DATA

Ananda Faridhatul Ulva
Sistem Informasi Universitas Malikussaleh Lhokseumawe
Jl. Cot Tgk Nie-Reulet, Aceh Utara, 141 Indonesiaemail :
anandafulva19@gmail.com(1)

Abstrak

Perkembangan teknologi semakin maju setiap zaman dengan berkembangnya teknologi kebutuhan manusia akan teknologi semakin besar terutama kebutuhan manusia dalam teknologi informasi. Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Algoritma kunci publik banyak digunakan karena kekuatan pengamanannya tapi memiliki kelemahan dalam lambatnya proses enkripsi dan dekripsi. Penggabungan proses enkripsi dengan menggunakan algoritma simetris yaitu Affine Cipher yang kemudian hasil dari affine cipher dienkripsi kembali dengan menggunakan Hill Cipher sehingga akan menutupi kelemahan dari Affine Cipher kemudian untuk menutupi kelemahan dari kedua algoritma dalam proses pengaman kunci digunakan algoritma asimetris atau algoritma kunci publik yaitu ElGamal sehingga nantinya memunculkan suatu kombinasi algoritma yang dapat memperkuat keamanan data

Kata Kunci : Kriptografi,Affine Chipper, Hill Chiper, ElGamal

1. Pendahuluan

Perkembangan teknologi semakin maju setiap zaman dengan berkembangnya teknologi kebutuhan manusia akan teknologi semakin besar terutama kebutuhan manusia dalam teknologi informasi. Di zaman sekarang dimana teknologi informasi berbasis komputer sudah berkembang sangat pesat dan sudah merupakan bagian dari kehidupan manusia yang tidak bisa dipisahkan. Dengan adanya kemajuan dalam teknologi informasi, komunikasi dan komputer maka akan muncul juga berbagi macam kejahatan baru dalam hal keamanan dalam penyampaian informasi. Masalah keamanan informasi merupakan aspek terpenting karena banyak pihak yang ingin merebut informasi atau data. Untuk

menghindari hal tersebut maka diperlukan sebuah teknik untuk menjaga informasi atau data dengan cara menyamarkan informasi yang dikirim ke dalam bentuk yang tidak dapat dibaca atau disebut cipherteks oleh pihak ketiga dan saat data itu sampai ke tangan pihak penerima data tersebut diubah lagi ke dalam bentuk yang bisa dibaca atau biasa yang disebut plainteks. Teknik atau ilmu inilah yang disebut dengan *cryphtography*.(Fairuzabadi, 2013)

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Pada zaman sekarang, kriptografi sudah menjadi bagian dasar dari keamanan komputer karena inti dari keamanan komputer adalah data ataupun informasi.Komputer merupakan sarana dalam mengirmkan data dan informasi ke jaringan untuk dikirim ke penerima, untuk itu data daninformasi yang dikirim tersebut harus diamankan agar orang yang tidak mempunyai hak akses tidak dapat melihat isi dari data dan informasi yang dikirim agar data yang dikirim sampai ke tangan penerima dengan selamat tanpa diketahui oleh pihak ketiga. Data atau informasi tersebut perlu diamankan dengan disamarkanmenggunakan teknik kriptograpfi sehingga orang lalin tidak dapat mengenali data yang dikirim.

Untuk mengamankan data atau informasi pada kriptografi terdapat dua proses dalam pengamanan data yaitu proses enkripsi dan dekripsi.Prosesenkripsi adalah proses dimana mengubah pesan asli atau biasa disebut *plaintext* menjadi pesan dalam bentuk yang tidak bisa dibaca atau tersandi yang biasa disebut *ciphertext*. Proses enkripsi akan menghasilkan data yang sudah tidak bisa dibaca oleh pihak yang tidak memiliki kepentingan dan data yang sudah dienkripsi hanya dapat dibuka atau dibaca oleh pihak penerima yang memiliki kunci (key) sedangkan proses dekripsi adalah proses untuk mengembalikan data yang sudah tersandi atau *ciphertext* tersebut menjadi data asli atau *plaintext*. (Fairuzabadi, 2013)

Berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi dua jenis yaitu kriptografi kunci simetris *(symmetric-key cryptography)* dan kriptografi kunci asimetris *(asymmetric-key cryptography).*(Munir, 2006).

Dalam dunia kriptografi kunci yang digunakan untuk mengenkripsi dan mendekripsi pesan menjadi satu elemen yang penting. Karena kunci yang menentukan cipherteks dapat dibaca oleh penerima atau tidak.

Karena itu dilakukan banyak cara untuk menjaga kerahasian kunci salah satunya adalah dikembangkannya algoritma kunci publik atau yang biasa disebut kriptografi kunci asimetris. (Wahyuni, 2011). Algoritma kunci publik banyak digunakan karena kekuatan pengamanannya tapi memiliki kelemahan dalam lambatnya proses enkripsi dan dekripsi. Oleh karena itu algoritma simetris masih banyak digunakan karena proses enkripsi dan dekripsinya cepat dan mudah dalam implementasinya tapi memiliki kelemahan dalam keamaan kunci. Maka untuk menutupi kelemahan masing-masing algoritma ada upaya untuk menggabungkan kedua algoritma yang dimana salah satu algoritma asimetris digunakan untuk mengamankan kunci dan algoritma simetris digunakan untk mengamankan pesan. Teknik untuk menggabungkan algoritma kunci asimetrisa dan simetris disebut dengan kriptografi hybrid atau juga disebut *Hybrid Cryptosystem* (Mantoro& Zakariya, 2012)

Dalam penggunaan algoritma hybrid, teknik enkripsi yang digunakan adalah kriptografi simetri dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *publickey cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi.

Affine Cipher adalah jenis algoritma cipher substitusi monoalphabetic dan affine cipher termasuk dalam kriptografi simetris dimana kunci yang digunakan dalam proses enkripsi dan dekripsi menggunakan kunci yang sama.Affine cipher memiliki kelemahan dalam frekuensi kemunculan huruf yang sama pada cipherteks. (Winata ,2012) Hill cipher merupakan algoritma kriptografi yang menggunakan perkalian matriks dan juga termasuk dalam algoritma kunci simetris seperti affine cipher. Hill cipher memiliki kelebihan dalam setiap karakter plainteks tidak selalu diubah menjadi karakter cipherteks yang sama.

Hal ini membuat orang lain mengalami kesulitan dalam memecahkan pesan jika mereka tidak bisa mengetahui metode apa yang digunakan. Selain itu Hill cipher memiliki kelebihan lain dalam banyaknya kemungkinan kunci yang diambil karena kunci yang diambil bisa matriks berapapun. (Ramadhan, 2015) Tetapi kedua algoritma ini memiliki kelemahan dalam masalah proses distribusi kunci. Karena itu dibutuhkan algoritma kunci publik yang digunakan untuk proses pengamanan kunci selama proses pengiriman ke pihak penerima.

Pada algoritma kriptografi asimetris ada algoritma yang mempunyai tingkat keamanan yang tinggi karena kompleksiotas algoritmanya yang terletak pada sulitnya perhitungan logaritma ketika bilangan yang dipilih

adalah bilangan prima yang bernilai besar algoritma tersebut adalah ElGamal. (Widyartno, 2011)

Berdasarkan latar belakang masalah diatas penulis mencoba melakukan penelitian untuk menggabungkan proses enkripsi dengan menggunakan algoritma simetris yaitu *Affine Cipher* yang kemudian hasil dari affine cipher dienkripsi kembali dengan menggunakan *Hill Cipher* sehingga akan menutupi kelemahan dari *Affine Cipher* kemudian untuk menutupi kelemahan dari kedua algoritma dalam proses pengaman kunci digunakan algoritma asimetris atau algoritma kunci publik yaitu *ElGamal* sehingga nantinya memunculkan suatu kombinasi algoritma yang dapat memperkuat keamanan data sehingga data yang dikirim lebih sulit untuk didekripsi dan cepat dalam proses enkripsinya. Serta penulis dalam hal ini dalam melakukan sebuah kombinasi tersebut untuk meningkatkan keamanan dari pesan, dimana diharapkan dari kombinasi ini mampu menangani isu keamanan data.

Bataasan permasalahan Metode kriptografi yang digunakan adalah *Affine Cipher, Hill Cipher*, dan *ElGamal*. Proses yang dilakukan adalah proses enkripsi dan dekripsi dalam bentuk teks. Algoritma *ElGamal* menggunakan kunci pembangkit bilangan prima hingga 255. Tidak diteliti bentuk serangan terhadap kriptografi. Pembangkitan bilangan acak menggunakan fungsi random yang sudah ada.

Berdasarkan latar belakang diatas dapat dirumuskan permasalahan yang akan diselesaikan yaitu bagaimana mengkombinasikan dan mengimplementasikan beberapa algoritma antara kriptografi kunci simetris *Affine Cipher* dan *Hill Cipher* dengan kriptografi kunci simetris ElGamal dalam meningkatkan keamanan sebuah sistem informasi, yang dapat meliputi kerahasian data, keabsahan data, integritas data, serta autentikasi data.

2.TINJAUAN PUSTAKA

2.1 Sistem dan Kriptografi

Kriptografi adalah ilmu yang menggunakan ilmu matematika untuk diguanakan dalam proses pengamanan informasi seperti kerahasiaan, integritas data serta otentikasi. *Cryptographic algorithm* adalah fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Terdapat dua fungsi yang saling berhubungan yaitu untuk enkripsi dan untuk dekripsi.

Dalam sistem juga terdapat algoritma untukmelihat aplikasi asmaul husna berbasis android (Fitriani, et all., 2017). Kemudian pengembangan dari sistem dapat dilihat dari aplikasi kompresi teks sms pada mobile device berbasis android dengan menggunakan algoritma huffman kanonik. (Dinata, 2016). Selanjutnya pengembangan dari sistem dapat diihat dalam machine learning dalam simulasi heat transfer flat-plate type solar collector (Ula et all., 2018).

Enkripsi merupakan proses penyandianuntuk mengubah sebuah pesan sehingga isi dari pesan tersebut tidak diketahui hasil dari pesanyang diubah disebut *ciphertext*. Dekripsi adalah proses untuk mengembalikan pesan yang disandi menjadi pesan asli. Sebuah sistem proses enkripsi dan dekripsi disebut *cryptosystem*.

Pada dasarnya kriptografi terdiri dari beberapa elemen seperti : (Ariyus, 2008):

1. Pesan, Plainteks dan Cipherteks.

Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Proses menyandikan plainteks menjadi cipherteks disebut enkripsi. Sedangkan proses mengembalikan cipherteks menjadi plainteks semula dinamakan dekripsi

2. *Cipher*

Algoritma kriptografi disebut juga *cipher* yaitu aturan untuk *enciphering* dan *deciphering*, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi.

3. Sistem kriptografi

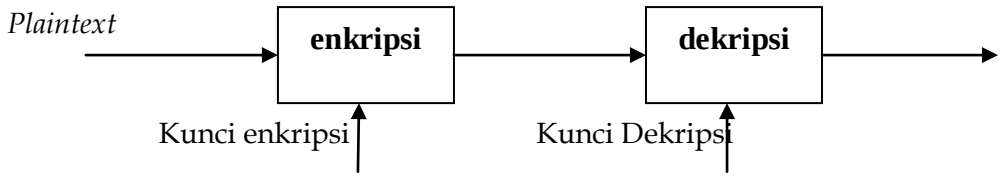
Sistem kriptografi merupakan kumpulan yang terdiri dari algoritma kriptografi, semua plainteks dan cipherteks yang mungkin dan kunci.

4. Penyadap

Penyadap adalah orang yang berusaha mencoba menangkap pesan selama ditransmisikan dengan tujuan mendapatkan informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan cipherteks.

5. Kriptanalisis dan kriptologi

Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Adapun alur dari proses enkripsi dan dekripsi pada kriptografi dapat dilihat pada gambar 1:

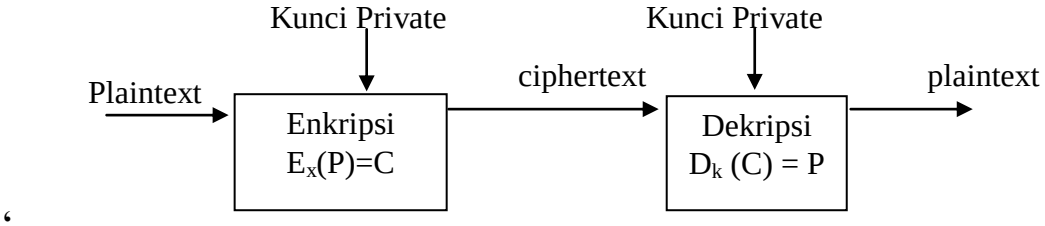


Gambar 1 Diagram proses enkripsi dan dekripsi

Algoritma simetrisatau disebut *juga secret key algorithm* adalahalgoritma yang kunci enkripsinya dapat dihitung dari kunci dekripsi dan begitupula sebaliknya, kunci dekripsi dapat dihitung dari kunci enkripsi. Pada sebagianbesar algoritma simetriskunci enkripsi dan kunci dekripsi adalah sama. algoritma simetrismemerlukan kesepakatan antara pengirim dan penerimapesan pada suatu kunci sebelum dapat berkomunikasi secara aman.

Mekanismenya dapat digambarkan melalui contoh sebagai berikut :

1. Budi dan Susi menyepakati suatu algoritma kriptografi.
2. Budi dan Susi menyepakati sebuah kunci
3. Budi mengambil plaintextnya dan mengenkripsikannya dengan menggunakan algoritma kriptografi dan kunci yang sudah disepakati.
4. Budi mengirimkan ciphertext tersebut kepada Susi
5. Susi mendekripsikan ciphertext tersebut dengan algoritma dan kunci yang sama. Susi kemudian mendapatkan plaintext dan membacanya. Adapaun proses enkripsi dan dekripsi pada algoritma simetris dapat dilihat pada gambar 2.2



‘

Gambar 2 Proses Enkripsi dan Dekripsi pada algoritma simetris

3. METODELOGI PENELITIAN

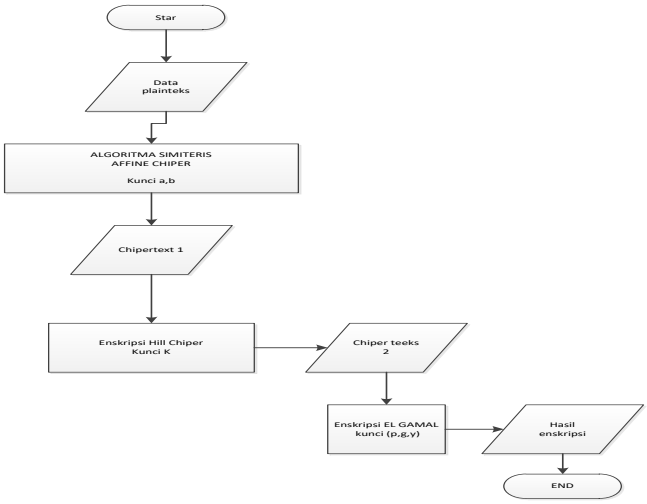
1. Pengumpulan Sumber data

Pengumpulan data yang digunakan dalam penelitian ini menggunakan studi literatur dan tinjauan pustaka, bahan-bahan penelitian dikumpulkan melalui berbagai sumber kepustakaan, baik berupa buku, jurnal, prosiding dan lain-lain sebagai bahan pendukung.

2. Subjek Penelitian

Subyek penelitian ini adalah penggabungan dari algoritma kriptografi*Affine Cipher, Hill Cipher* dan ElGamal dalam penyandian data, sehingga nantinya dari algoritma yang dikombinasi akan menghasilkan algoritma yang baru yang mempunyai tingkat kesulitan pengamanan data yang tinggi dan cepat dalam proses enkripsi maupun dekripsi.

3. Perancangan Sistem



Gambar 3 Skema perancangan system

4. Hasil dan Implementasi

1. Alur Proses Enksripsi pesan oleh pengirim

Pada proses enkripsi pesan, plainteks dimisalkan ZULKIFLI dienkripsi terlebih dahulu dengan menggunakan algoritma menggunakan algoritma *Affine Cipher* dengan menggunakan kunci *affine* menghasilkan cipherteks 1, kemudian cipherteks 1 dienkripsi lagi dengan algoritma *Hill*

*Cipher*sehingga menghasilkan cipherteks 2.Chiperteks 2 atau cipherteks hasil dari enkripsi *hill cipher* misalkan LMONE yang dikirim ke penerima.
Pengujian *Plainteks*

Tabel 1. Teks Input Plainteks

Z	U	L	K	I	F	L	I
25	20	11	10	8	5	11	8

Plainteks
ZULKIFLI
Ekivalen :
25 20 11 10 8 5 11 8
N = 26
K = Relatif Prima (1,3,5,7,9,11,15,17,19,21,23, 25)
Kunci pertama = 5
Kunci kedua 7

Affine Chiper dengan mengambil m = 5 (karena 5 relatif prima dengan 26) dan b = 7. Karena alphabet yang diguanakn 26 huruf, maka n = 26. Enskripsi palinteks dihitung dengan kekongurenan :

$$C = 5P + 7 \ (mod\ 26)$$

Perhitungannya adalah sebagai berikut :
P1 = 25 → C1 = 5.25 + 7 = 132 (mod 26) = 2 = C
P2 = 20 → C2 = 5.20 + 7 = 107 (mod 26) = 3 = D
P3 = 11 → C3 = 5.11 + 7 = 62 (mod 26) = 10 = K
P4 = 10 → C4 = 5.10 + 7 = 57 (mod 26) = 5 = F
P5 = 8 → C5 = 5.8 + 7 = 47 (mod 26) = 21 = V
P6 = 5 → C6 = 5.5 + 7 = 32 (mod 26) = 6 = G
P7 = 11 → C7 = 5.11 + 7 = 62 (mod 26) = 10 = K
P8 = 8 → C8 = 5.8 + 7 = 47 (mod 26) = 21 = V

Maka menghasilkan chiperteks1 = C D K F V G K V
Setelah didapatnya hasil chiperteks1 maka selanjutnya akan melakukan proses enskripsi dengan Hill Chiper dimana plainteks 2 = chiperteks 1
Hill Cipher merupakan salah satu algoritma kriptografi kunci simetris. Algoritma *Hill Cipher* menggunakan matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang

digunakan dalam *Hill Cipher* antara lain adalah perkalian antar matriks dan melakukan invers pada matriks.

Dengan matriks kunci $k = \begin{matrix} 4 & 3 \\ 3 & 3 \end{matrix}$

Tabel 2. Teks Inputplainteks 2 hasil dari enskripsi *Affine Chiper*

C	D	K	F	V	G	K	V
2	3	10	5	21	6	10	21

Plainteks 2 : CDKFVGKV

Ekivalen = 2 3 10 5 21 6 20 21

Kunci k = $\begin{matrix} 4 & 3 \\ 3 & 3 \end{matrix}$

Langkah selanjutnya adalah membagi deretan angka tadi menjadi blok matirks yang sesuai dengan jumlah kolom matriks kunci (2)

Pembagian blok

CD = $\begin{matrix} 2 \\ 3 \end{matrix}$ KF = $\begin{matrix} 10 \\ 5 \end{matrix}$ VG = $\begin{matrix} 21 \\ 6 \end{matrix}$ KV = $\begin{matrix} 10 \\ 21 \end{matrix}$

Memulai proses enskripsi (Matriks kunci * blok matirk (plainteks))

C1 (CD) = $\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 17 \\ 15 \end{bmatrix} (mod\ 26) = \begin{bmatrix} 17 \\ 25 \end{bmatrix}$

C2 (KF) = $\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 10 \\ 5 \end{bmatrix} = \begin{bmatrix} 55 \\ 45 \end{bmatrix} (mod\ 26) = \begin{bmatrix} 3 \\ 19 \end{bmatrix}$

C3 (VG) = $\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 21 \\ 6 \end{bmatrix} = \begin{bmatrix} 102 \\ 81 \end{bmatrix} (mod\ 26) = \begin{bmatrix} 24 \\ 3 \end{bmatrix}$

C4 (KV) = $\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 10 \\ 21 \end{bmatrix} = \begin{bmatrix} 103 \\ 93 \end{bmatrix} (mod\ 26) = \begin{bmatrix} 25 \\ 15 \end{bmatrix}$

Maka Chiperteks 2 adalah 17 25 3 19 24 3 25 15 = R Z D T Y D Z P

4. Alur Proses Deskripsi Pesan oleh Penerima

Pada proses dekripsi pesan, chiperteks yang dikirimoleh pengirim LMONE didekripsi lagi oleh penerima, pertama cipherteks dienkripsi dengan menggunakan algoritma hill cipher menghasilkan cipherteks 1, kemudian pesan didekripsi menggunakan Affine Cipher menghasilkan plainteks.

Memulai proses deskripsi (invers matriks kunci *blok matriks(chipper text)). Langkah pertama adalah mencari invers matriks kunci menggunakan invers modulo determinan matriks kunci.

K = $\begin{bmatrix}4 & 3\\3 & 3\end{bmatrix}$ → determinan k = (4*3)-(3*3) = 3

Invers modulo

3^{-1} mod 26 → 3x = 1 mod 26 → 3x = 1 + 26k → x = (1+26 k)/3

Cari k =n sehingga hasil x adalah bilangan bulat dimana k=0 →

X=(1+26*1)/3 = 9 (bilangan bulat). Sehingga invers dari 3 mod 26 ekivalen dengan 9 mod 26 yaitu 9

Invers modulo determinan digunakan untuk mencari invers matriks yaitu

Missal k = $\begin{bmatrix}a & b\\c & d\end{bmatrix}$ maka k^{-1} = determinan $\begin{bmatrix}d & -b\\-c & a\end{bmatrix}$

Sehinga :

$k^{-1} = 9\begin{bmatrix}3 & -3\\-3 & 4\end{bmatrix} = \begin{bmatrix}27 & -27\\-27 & 36\end{bmatrix} mod\ 26 = \begin{bmatrix}1 & 25\\25 & 10\end{bmatrix}$

Dimana chipertks yang akan dideskripsi terlihat pada Tabel 3

Tabel 3. Chiperteks 2 yang akan dideskripsi dengan kuncil Hill chiper

R	Z	D	T	Y	D	Z	P
17	25	3	19	24	3	25	15

Sehingga akan dibagi 2 yaitu

RZ = $\begin{bmatrix}17\\25\end{bmatrix}$ DT = $\begin{bmatrix}3\\19\end{bmatrix}$ YD = $\begin{bmatrix}24\\3\end{bmatrix}$ ZP = $\begin{bmatrix}25\\15\end{bmatrix}$

Alur proses deskripsinya menggunakan kunci *hill chipper* yaitu

P1(RZ) = $\begin{bmatrix}1 & 25\\25 & 10\end{bmatrix}\begin{bmatrix}17\\25\end{bmatrix} = \begin{bmatrix}642\\675\end{bmatrix} mod\ 26 = \begin{bmatrix}2\\3\end{bmatrix}$

P2(DT) = $\begin{bmatrix}1 & 25\\25 & 10\end{bmatrix}\begin{bmatrix}3\\19\end{bmatrix} = \begin{bmatrix}478\\265\end{bmatrix} mod\ 26 = \begin{bmatrix}10\\5\end{bmatrix}$

P3(YD) = $\begin{bmatrix}1 & 25\\25 & 10\end{bmatrix}\begin{bmatrix}24\\3\end{bmatrix} = \begin{bmatrix}99\\630\end{bmatrix} mod\ 26 = \begin{bmatrix}21\\6\end{bmatrix}$

P4 (ZP) = $\begin{bmatrix}1 & 25\\25 & 10\end{bmatrix}\begin{bmatrix}25\\15\end{bmatrix} = \begin{bmatrix}400\\775\end{bmatrix} mod\ 26 = \begin{bmatrix}10\\21\end{bmatrix}$

Hasil deskripsi = 2 3 10 5 21 6 10 21 = C D K F V G K V

Dapat dilihat menandakan hasil deskripsi chipper teks menghasilkan plainteks (chiperteks 1) yang menandakan berarti pengerjaan diatas sudah benar. Untuk langkah selanjutanya hasil deksripsi dari *Hill chipper* akan dideskripsi menggunakn kunci *affine chipper* untuk melihatkan hasil yang sebenarnya.

Proses deskripsi menggunakan kunci *affine chipper* adalah sebagai berikut :

Tabel 4. Teks inputan plainteks mengunakan kunci *affine chipper*

C	D	K	F	V	G	K	V
2	3	10	5	21	6	10	21

Chipper teks1 = C D K F V G K V
Ekivalen = 2 3 10 5 21 6 10 21
N = 26
K = relative prima (1,3,5,7,11,15,17,19,21,23,25)
Kunci pertama = 5
Kunci kedua = 7

Untuk mengembalikan teks yang telah dienskripsi menjadi pesan rahasia dapat dilakukan dengan proses deksripsi, pertama dapat dihitung 5^{-1}(mod 26) yang dapat dihitung dengan memecahkan kekongurenan lanjar

5x =1 (mod 26)(7)
Untuk deskripsi dengan hasil 1 maka solusinya adalah x = 21 (mod 26) dikarenakan 5.21 = 105 mod 26 = 1, maka untuk proses deksripsinya adalah P = 21 (C-7)(mod 26)(8)

P1 =2 → c1 = 21 (2-7) = (-105) (mod 26) = 25
P2 = 3 → c2 = 21 (3-7) = (-84) mod 26) = 20
P3 10 → c3 = 21 (10-7) =(63) mod 26 = 11
P4 = 5 → c4 = 21 (5-7) = 42 (mod 26) = 10
P5 = 21 → c5 = 21 (21-7) = 294 (mod 26) = 8
P6 = 6 → c6 = 21 (6-7) = 21 (mod 26) = 5
P7 = 20 → c7 = 21 (11-7) = 84 (mod 26) = 11
P8 = 21 → c8 = 21 (21-7) = 294 (mod 26) = 8
Maka menghasilkan plainteks Z U L K I F L I

5. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian ini adalah :

1. Algoritma kriptografi penggabuangan simetris dan asimetris, ini sangat baik ditambah menggunakan algoritma asimetris El gamal yang sangat baik untuk mengatasi masalah distirbusi kunci
2. Pengunnaan algoritma menggunakan algoritma *Affine Cipher* dengan menggunakan kunci *affine* menghasilkan cipherteks 1, kemudian cipherteks 1 dienkripsi lagi dengan algoritma *Hill Cipher* sehingga menghasilkan cipherteks 2.
3. Pada algoritma El Gamal, proses enksirpsi pada plainteks yang sama akan diperoleh chipperteks yang berbeda-beda, namun pada proses deskripsi diperoleh kembali plainteks yang sama.

6. Saran

Kombinasi beberapa metode pada kriptografi Seperti cipher transposisi menambah tingkat kesulitan dari kriptografi ini.

DAFTAR PUSTAKA

Ariyus, D. 2008. Pengantar Ilmu Kriptografi; Teori, analisis dan implementasi. ANDI OFFSET. Yogyakarta.

Dinata, R. K., & Hasmar, M. A. H. (2019). Aplikasi Kompresi Teks Sms Pada Mobile Device Berbasis Android Dengan Menggunakan Algoritma Huffman Kanonik. TECHSI-Jurnal Teknik Informatika, 8(2), 44-53.

Batten, L, M. 2013. *Public key Cyrptography : Application and Attacks*. IEEE Press. Australia

Fauzana. 2013. Analisis dan Perancangan sistem autentifikasi penggunaan pada web menggunakan metode multiple-key RS4. Skripsi. Universitas Sumatera Utara. Medan.

Fitrianti, U., & Ula, M. (2017). Implementasi algoritma levenshtein distance dan algoritma knuth morris pratt pada aplikasi asmaul husna berbasis android. Jurnal Sistem Informasi, 1(2).

Katz, L and Lindell, Y. 2007. *Introduction* to Modern Cyrptogtahphy Chapman & Hall/CRC. United States

Kromodimoeljo, S. 2009. Teori dan Aplikasi Kriptografi. SPK IT Consulting. Jakarta.

Munir, R. 2006. Kriptografi. Informatika. Bandung

.Smart, N. 2004. Cyrptography : An Introduction. 3rd Edition. University of Bristol.

Wirdasari, D. 2008. Prinsip Kerja Kriptografi dalam mengamankan Informasi. Jurnal Saintikom Vol 5 (2). Kudus

Ula, M., Darnila, E., & Siagian, P. (2018, June). Numerical simulation of styrofoam and rockwool heat transfer flat-plate type solar collector. IOP Conference Series: Material Science and Engineering.