Jurnal Riset Mahasiswa Matematika
Volume 2(6) (2023), Pages 247-256
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Penggabungan Metode Vigènere Cipher dan ElGamal Pada Pengamanan Pesan Rahasia

Ludyawati, Muhammad Khudzaifah, Erna Herawati

Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia

ludyawt@gmail.com*, khudzaifah@uin-malang.ac.id, faridatul_mahya@uin-malang.ac.id

Abstrak

Vigènere Cipher adalah salah satu kriptografi algoritma simetris yang menggunakan satu jenis kunci yang sama pada proses enkripsi dan dekripsi. Keamanan dari metode *Vigènere Cipher* terletak pada perhitungan modulo yang digunakan. ElGamal adalah salah satu kriptografi algoritma asimetris yang menggunakan dua jenis kunci yang berbeda pada proses enkripsi dan dekripsi. Keamanan dari algoritma ElGamal adalah terletak pada kerumitan perhitungan bilangan prima besar. *Vigènere Cipher* dan ElGamal memiliki kelebihan dan kekurangan masing-masing. Oleh karena itu peneliti tertarik untuk mengkombinasikan kelebihan dari dua metode tersebut. Pada penelitian ini dilakukan dua kali penguncian pada proses enkripsi dan dekripsi. Pada proses enkripsi menggunakan kunci publik dan pada proses dekripsi menggunakan kunci publik (p, a, β) dan kunci rahasia (d). Kunci yang digunakan berasal dari pembentukan kunci menggunakan algoritma ElGamal. Keamanan kunci yang dibentuk dari algoritma ElGamal terletak pada bilangan prima besar aman p, akar primitif a dari bilangan prima p, dan bilangan bulat acak d yang berasal dari tiga digit terakhir dari Nomor Induk Mahasiswa. Kesimpulan dari penelitian ini adalah kombinasi dari metode *Vigènere Cipher* dan ElGamal dapat meningkatkan keamanan pesan rahasia karena menghasilkan cipherteks dengan ukuran dua kali lipat (γ, δ) dari pesan asli.

Kata Kunci: enkripsi; dekripsi; *vigènere cipher*; elgamal

Abstract

Vigènere Cipher is a symmetric cryptographic algorithm that uses the same type of key in the encryption and decryption process. The security of the Vigènere Cipher method lies in the modulo calculation used. ElGamal is an asymmetric cryptographic algorithm that uses two different types of keys in the encryption and decryption process. The security of the ElGamal algorithm lies in the complexity of calculating large prime numbers. The Vigènere Cipher and ElGamal have their advantages and disadvantages. The researchers are interested in combining the advantages of the two methods. In this study, two locks were carried out in the encryption and decryption process. The encryption process uses a public key and the decryption process uses a public key (p, a, β) and a secret key (d). The key used comes from key formation using the ElGamal algorithm. The key security formed from the ElGamal algorithm lies in the large prime p, the primitive root a of the prime number p, and the random integer d which comes from the last three digits of Student Number. The conclusion of this study is that the combination of the Vigènere Cipher and ElGamal methods can increase the security of secret messages because it produces a ciphertext with twice the size (γ, δ) of the original message.

Keywords: encryption; decryption; vigènere cipher; elgamal.

PENDAHULUAN

Pada era saat ini, informasi menjadi aset beharga yang harus dilindungi. Jatuhnya informasi ke pihak tidak terkait menjadi ancaman yang cukup serius bagi semua pihak, tidak terkecuali pihak penting seperti pemerintahan, militer, perbankan, pendidikan, dan lain-lain. Bagi pihak-pihak tersebut faktor utama yang harus terpenuhi dalam mengirim pesan rahasia adalah

Submitted: 12 Agustus 2022 Reviewed: 20 April 2023 Accepted: 26 Agustus 2023
Doi: http://dx.doi.org/10.18860/jrmm.v2i6.22041

tingkat keamanan informasi. Cara untuk meningkatkan keamanan informasi adalah dengan menggunakan Kriptografi. Kriptografi memiliki 2 algoritma yang didasarkan pada kuncinya, diantaranya Algoritma simetris (*symmetric-key cryptography*) dan algoritma asimetris (*asymmetric-key cryptography*) [1]. Algoritma simetris memiliki satu jenis kunci yang digunakan untuk proses enkripsi dan proses dekripsi. Sedangkan untuk algoritma asimetris memiliki dua jenis kunci yaitu kunci publik dan kunci rahasia [2].

Salah satu contoh dari algoritma simetris adalah metode *Vigenère cipher*. *Vigenère cipher* pertama kali dipublikasikan oleh *Blaisè de Vigenère* seorang diplomat Prancis sekaligus kriptologis pada abad 16 yaitu tahun 1586 [1]. Digambarkan pertama kali oleh Giovian Batista Belaso pada tahun 1553 pada bukunya yang berjudul *La Cifra del Sig*. Ide dasar dari metode ini adalah sama seperti metode *Caesar cipher*, akan tetapi jumlah pergeseran tiap huruf berbeda-beda. Untuk mengenkripsi pesan rahasia biasanya dapat menggunakan *tabula recta* [2].

Berikutnya salah satu contoh algoritma asimetris adalah ElGamal. Algoritma ini pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985 [3]. Algoritma ElGamal ini pada awalnya digunakan untuk *digital signature*, akan tetapi kemudian dimodifikasi untuk melakukan enkripsi dan dekripsi pesan [1]. Keamanan dari algoritma ElGamal ini terletak pada rumitnya perhitungan logaritma diskrit pada bilangan modulo prima yang besar sehingga upaya untuk melakukan pembobolan menjadi sangat sukar [4].

Pada tahun 2018 Bella Ariska, Suroso, dan Jon Endri melakukan penelitian yang berjudul "Rancangan Kriptografi Hybrid Kombinasi Metode Vigènere Cipher dan Elgamal pada Pengamanan Pesan Rahasia". Kesimpulan yang didapat pada penelitian tersebut adalah bahwa kombinasi kedua metode tersebut dapat melakukan dapat melakukan proses enkripsi dan dekripsi pesan rahasia serta mempunyai kemampuan yang baik dalam mengatasi masalah pada proses pendistribusian kunci [5]. Pada tahun 2017 Divananda Zikry Fadilla melakukan penelitian dengan judul "Implementasi Algoritma ElGamal dan Vigènere Cipher untuk Enkripsi dan Dekripsi Data Citra Digital". Kesimpulan yang didapat pada penelitian tersebut adalah dua kombinasi tersebut dapat melakukan enkripsi dan dekripsi pada citra atau gambar [6].

METODE

Langkah-langkah Penelitian

1. Proses pembentukan Kunci

Membentuk kunci publik dan kunci rahasia. Pembentukan kunci ini menggunakan Algoritma ElGamal. Untuk membentuk kunci publik dan rahasia dibutuhkan bilangan acak, bilangan prima, dan akar primitif [15]. Untuk bilangan bulat acak dipilih melalui 3 angka terakhir pada NIM. Pada proses menentukan bilangan prima, bilangan prima dapat dikatakan bilangan prima aman jika memenuhi syarat:

a. Pilih bilangan prima $\boldsymbol{p}$ dengan syarat $\mathbf{100} < \boldsymbol{p} < \mathbf{999}$ [7]. Pemilihan bilangan prima $\boldsymbol{p}$ dapat dilakukan secara acak menggunakan *software Python*.
b. Melakukan pengecekan bilangan prima aman dengan menggunakan perhitungan $\boldsymbol{q}$ yaitu $\boldsymbol{p} = \mathbf{2}\boldsymbol{q} + \mathbf{1}$ [8]. Jika $\boldsymbol{q}$ merupakan bilangan prima, maka $\boldsymbol{p}$ merupakan bilangan prima aman. Jika $\boldsymbol{q}$ bukan merupakan bilangan prima, maka $\boldsymbol{p}$ bukan merupakan bilangan prima aman.
c. Menentukan $\boldsymbol{\alpha}$ dengan catatan $\boldsymbol{\alpha} \in \mathbb{Z}_{\boldsymbol{p}}^{*}$. Untuk menentukan akar primtif acak ini dapat dilakukan dengan menggunakan bilangan yang relatif prima dengan $\boldsymbol{p}$ atau dipilih secara acak menggunakan software Python.
d. Melakukan pengecekan dengan menggunakan perhitungan $\boldsymbol{\alpha^2 mod\ p}$ dan $\boldsymbol{\alpha^q mod\ p}$ [8]. Jika $\boldsymbol{\alpha^2 mod\ p} = \mathbf{1}$ dan $\boldsymbol{\alpha^q mod\ p} = \mathbf{1}$, maka $\boldsymbol{\alpha}$ adalah bukan akar primitif. Jika $\boldsymbol{\alpha^2 mod\ p} \neq \mathbf{1}$ dan $\boldsymbol{\alpha^q mod\ p} \neq \mathbf{1}$, maka $\boldsymbol{\alpha}$ adalah akar primitif.

2. Proses Enkripsi Pesan
   a. Menetukan pesan asli atau plainteks yang digunakan
   b. Proses enkripsi tahap pertama ini dilakukan dengan menggunakan modifikasi perhitungan modulo dalam metode *Vigènere Cipher*, yaitu dengan menggunakan modulo

ASCII *printable*[9]. Proses enkripsi tahap pertama ini menghasilkan cipherteks yang berupa angka.

c. Langkah selanjutnya adalah melakukan proses enkripsi tahap kedua pada cipherteks yang telah didapatkan dari proses enkripsi tahap pertama menggunakan algoritma ElGamal. Pada proses enkripsi tahap kedua ini diperlukan bilangan acak yang didapatkan melalui *Microsoft Excel*. Proses enkripsi tahap kedua ini menghasilkan cipherteks yang berupa pasangan angka .

d. Selanjutnya pengirim mengirimkan kunci publik kepada penerima untuk proses deksripsi pesan rahasia.

3. Proses Dekripsi Pesan

a. Setelah menerima pesan, langkah selanjutnya adalah proses dekripsi tahap pertama menggunakan metode ElGamal. Dalam proses dekripsi tahap pertama ini membutuhkan kunci rahasia yang telah didapatkan dan bilangan acak yang didapatkan melalui *Microsoft Excel*. Pada proses dekripsi tahap pertama ini menghasilkan plainteks yang berupa angka.

b. Melakukan proses deksripsi tahap kedua pada plainteks yang telah didapatkan pada tahap pertama menggunakan metode *Vigènere Cipher*. Dalam proses dekripsi tahap kedua ini dilakukan dengan menggunakan modifikasi perhitungan modulo dalam metode *Vigènere Cipher*, yaitu dengan menggunakan modulo ASCII *printable* [9]. Proses dekripsi tahap kedua ini menggunakan kunci publik.

c. Mengubah plainteks yang didapatkan menjadi karakter berdasarkan tabel ASCII *printable*.

HASIL DAN PEMBAHASAN

1. Simulasi Pembentukan Kunci

a. Penentuan bilangan prima p aman yang bernilai besar [4]. Tujuan penentuan bilangan prima aman ini adalah untuk mempermudah dalam penentuan akar primitive [14]. Bilangan prima p dengan interval $100 < p < 999$ atau 3 digit [7]. Pemilihan bilangan prima p dapat dilakukan secara acak dengan menggunakan bantuan *software Python*. Dipilih $p = 827$

b. Melakukan pengecekan bilangan prima aman p [8].

$$\begin{aligned} p &= 2q + 1 \\ 827 &= 2q + 1 \\ 2q &= 827 - 1 \\ q &= \frac{826}{2} \\ q &= 413 \end{aligned}$$

Karena $q = 413$ adalah bilangan prima, maka p merupakan bilangan prima aman.

c. Menentukan $\boldsymbol{\alpha}$ dengan catatan $\boldsymbol{\alpha} \in \mathbb{Z}_{\boldsymbol{p}}^{*}$. Untuk menentukan akar primtif acak ini dapat dilakukan dengan menggunakan bilangan yang relatif prima dengan p atau menggunakan bantuan *software Python*. Berdasarkan definisi Euler untuk mencari akar primitif dapat dilakukan dengan perhitungan berikut [10].

$$\varphi(827) = \varphi(\varphi(827)) = \varphi(827 - 1) = 826$$

Dipilih $\alpha = 37$, karena $\gcd(37, 826) = 1$. Oleh karena itu 37 relatif prima dengan 826.

d. Untuk memastikan 37 adalah akar primitif dari perlu dilakukan pengecekan terhadap 827 dengan menggunakan perhitungan $\alpha^2 mod\ p$ dan $\alpha^q mod\ p$ [8].

- $\alpha^2 mod\ p$

$$\begin{aligned} \alpha^2 mod\ p &= 37^2 mod\ 827 \\ &= 1369\ mod\ 827 \\ &= 524 \end{aligned}$$

- $\alpha^q mod\ p$

$$\begin{aligned} \alpha^q mod\ p &= 37^{413} mod\ 827 \\ &= 826 \end{aligned}$$

Karena $\alpha^2 mod\ p \neq 1$ dan $\alpha^q mod\ p \neq 1$, maka 37 termasuk akar primitif dari $\mathbb{Z}_{827}^*$

e. Pilih bilangan bulat acak d, berdasarkan penggabungan 3 bilangan terakhir pada NIM atau nomor identitas mahasiswa.
NIM yang digunakan adalah 19610036. Sehingga 3 bilangan terakhir NIM tersebut adalah 036. Berdasarkan aturan yang telah ditetapkan maka $d = 36$.

f. Pembentukan kunci berdasarkan bilangan prima dan akar primitif.
Untuk mencari nilai β menggunakan perhitungan $\beta = \alpha^d mod\ p$ [3].

$$\begin{aligned} \beta &= \alpha^d mod\ p \\ &= 37^{36} mod\ 827 \\ &= 276 \end{aligned}$$

Diperoleh kunci publik (p, α, β) dan kunci rahasia (p, d)

g. Sehingga didapatkan kunci publik $(p, \alpha, \beta) = (827, 37, 276)$ dan kunci rahasia $(p, d = 827, 36)$.

2. Simulasi Enkripsi Pesan

a. Menentukkan plainteks atau pesan asli
Pada penelitian ini pesan asli atau (plainteks)-nya yang digunakan adalah Ludyawati-19610036. Peneliti memilih Plainteks tersebut karena berdasarkan nama lengkap serta nomor induk mahasiswa (NIM) dari peneliti. Plainteks tersebut dapat dirubah sesuai dengan kebutuhan dan keinginan penelitian selanjutnya.

b. Menentukkan indeks karakter dari plainteks yang telah dibuat

Tabel 1. Indeks Plainteks

Plainteks	Indeks	Plainteks	Indeks
L	76	-	45
u	117	1	49
d	100	9	57
y	121	6	54
a	97	1	49
w	119	0	48
a	97	0	48
t	116	3	51
i	105	6	54

c. Menentukkan indeks karakter dari kunci publik $(827, 37, 276)$

Tabel 2. Indeks Kunci

Kunci	Indeks	Kunci	Indeks
8	56	,	44
2	50	2	50
7	55	7	55
,	44	6	54
3	51		
7	55		

d. Melakukan Enkripsi Tahap Pertama dengan metode *Vigènere Cipher*.
Proses Enkripsi tahap pertama ini dilakukan dengan menggunakan modifikasi perhitungan modulo dalam metode *Vigènere Cipher*, yaitu dengan menggunakan modulo ASCII *printable* [9]. Proses enkripsi tahap pertama dilakukan dengan menggunakan perhitungan berikut [9]:

$$C_i = ((P_i + K_i - 32) mod\ 95) + 32$$

Sehingga proses enkripsi tahap kedua adalah sebagai berikut:

Tabel 3. Proses Enkripsi Tahap Pertama

i	Plainteks	Kunci	$E = ((P_i + K_i - 32) mod\ 95) + 32$	Cipherteks
1	76	56	$((76 + 56 - 32) mod\ 95) + 32$	37
2	117	50	$((117 + 50 - 32) mod\ 95) + 32$	72
3	100	55	$((100 + 55 - 32) mod\ 95) + 32$	60
4	121	44	$(121 + 44 - 32) mod\ 95) + 32$	70
5	97	51	$((97 + 51 - 32) mod\ 95) + 32$	53
6	119	55	$((119 + 55 - 32) mod\ 95) + 32$	79
7	97	44	$((97 + 44 - 32) mod\ 95) + 32$	46
8	116	50	$((116 + 50 - 32) mod\ 95) + 32$	71
9	105	55	$((105 + 55 - 32) mod\ 95) + 32$	65
10	45	54	$((45 + 54 - 32) mod\ 95) + 32$	99
11	49	56	$((49 + 56 - 32) mod\ 95) + 32$	105
12	57	50	$((57 + 50 - 32) mod\ 95) + 32$	107
13	54	55	$((54 + 55 - 32) mod\ 95) + 32$	109
14	49	44	$((49 + 44 - 32) mod\ 95) + 32$	93
15	48	51	$((48 + 51 - 32) mod\ 95) + 32$	99
16	48	55	$((48 + 55 - 32) mod\ 95) + 32$	103
17	51	44	$((51 + 44 - 32) mod\ 95) + 32$	95
18	54	50	$((54 + 50 - 32) mod\ 95) + 32$	104

e. Melakukan Enkripsi Tahap Kedua dengan Algoritma ElGamal.
Pada proses enkripsi tahap kedua kunci yang digunakan adalah kunci publik $(p, \alpha, \beta) = (827, 37, 276)$.. Dalam proses tahap kedua cipherteks didapatkan melalui (γ_i, δ_i) dengan menggunakan perhitungan enkripsi algoritma ElGamal yaitu sebagai berikut [3]:

$$\gamma = \alpha^k mod p \qquad \delta = \beta^k \cdot m_i mod p$$

Pada proses ini juga dibutuhkan bilangan bulat acak k yang berasal dari *Microsoft Excel* dengan aturan $1 \leq k \leq p - 1$ [13]. Notasi m adalah cipherteks yang telah didapatkan dari proses Enkripsi tahap pertama, sehingga proses enkripsi tahap kedua sebagai berikut:

Tabel 4. Proses Enkripsi Tahap Kedua

i	m_i	k_i	$\gamma_i = 37^{k_i} mod\ 827$	γ_i	$\delta_i = 276^{k_i} \cdot m_i mod\ 827$	δ_i

1	37	173	$37^{173} mod\ 827$	345	$276^{173} \cdot 37\ mod\ 827$	384
2	72	251	$37^{251} mod\ 827$	280	$276^{251} \cdot 72\ mod\ 827$	45
3	60	799	$37^{799} mod\ 827$	451	$276^{799} \cdot 60\ mod\ 827$	70
4	70	525	$37^{525} mod\ 827$	24	$276^{525} \cdot 70\ mod\ 827$	813
5	53	797	$37^{797} mod\ 827$	631	$276^{797} \cdot 53\ mod\ 827$	143
6	79	728	$37^{728} mod\ 827$	496	$276^{728} \cdot 79\ mod\ 827$	372
7	46	447	$37^{447} mod\ 827$	384	$276^{447} \cdot 46\ mod\ 827$	769
8	71	790	$37^{790} mod\ 827$	3	$276^{790} \cdot 71\ mod\ 827$	805
9	65	821	$37^{821} mod\ 827$	709	$276^{821} \cdot 65\ mod\ 827$	82
10	99	269	$37^{269} mod\ 827$	746	$276^{269} \cdot 99\ mod\ 827$	671
11	105	256	$37^{256} mod\ 827$	306	$276^{256} \cdot 105\ mod\ 827$	729
12	107	418	$37^{418} mod\ 827$	820	$276^{418} \cdot 107\ mod\ 827$	579
13	109	770	$37^{770} mod\ 827$	93	$276^{770} \cdot 109\ mod\ 827$	715
14	93	543	$37^{543} mod\ 827$	442	$276^{543} \cdot 93\ mod\ 827$	504
15	99	494	$37^{494} mod\ 827$	504	$276^{494} \cdot 99\ mod\ 827$	31
16	103	184	$37^{184} mod\ 827$	273	$276^{184} \cdot 103\ mod\ 827$	513
17	95	266	$37^{266} mod\ 827$	108	$276^{266} \cdot 95\ mod\ 827$	18
18	104	65	$37^{65} mod\ 827$	218	$276^{65} \cdot 104\ mod\ 827$	190

f. Cipherteks yang dihasilkan dari enkripsi tahap kedua ini berbentuk pasangan angka(γ_i, δ_i). Cipherteks yang telah dihasilkan ditunjukkan sebagai berikut:

Tabel 5. Cipherteks yang Dihasilkan

C1	(345, 384)	C7	(384, 805)	C13	(93, 715)
C2	(280, 45)	C8	(3, 805)	C14	(442, 504)
C3	(451, 70)	C9	(709, 82)	C15	(504, 31)
C4	(24, 813)	C10	(746, 671)	C16	(273, 513)
C5	(631, 143)	C11	(306, 729)	C17	(108, 18)
C6	(496, 372)	C12	(820, 579)	C18	(218, 190)

3. Simulasi Dekripsi Pesan

a. Proses dekripsi dimulai dengan proses dekripsi tahap pertama. Proses dekripsi tahap pertama menggunakan metode ElGamal dan kunci rahasia [12]. Kunci rahasia yang digunakan dalam penelitian ini adalah $(p, d = 827, 36)$. Proses dekripsi tahap pertama dilakukan menggunakan perhitungan [11]:

$$m_i = \delta_i \cdot \gamma_i^{(827-1-36)} mod\ 827$$

Berikut adalah proses dekripsi tahap pertama:

Tabel 6. Proses Dekripsi Tahap Pertama

i	γ_i	δ_i	$m_i = \delta_i \cdot \gamma_i^{(790)} mod\ 827$	m_i
1	345	384	$384 \cdot 345^{(790)} mod\ 827$	37
2	280	45	$45 \cdot 280^{(790)} mod\ 827$	72
3	451	70	$70 \cdot 451^{(790)} mod\ 827$	60
4	24	813	$813 \cdot 24^{(790)} mod\ 827$	70
5	631	143	$143 \cdot 631^{(790)} mod\ 827$	53
6	496	372	$372 \cdot 496^{(790)} mod\ 827$	79
7	384	769	$769 \cdot 384^{(790)} mod\ 827$	46
8	3	805	$805 \cdot 3^{(790)} mod\ 827$	71
9	709	82	$82 \cdot 709^{(790)} mod\ 827$	65
10	746	671	$671 \cdot 746^{(790)} mod\ 827$	99
11	306	729	$729 \cdot 306^{(790)} mod\ 827$	105
12	820	579	$579 \cdot 820^{(790)} mod\ 827$	107
13	93	715	$715 \cdot 93^{(790)} mod\ 827$	109
14	442	504	$504 \cdot 442^{(790)} mod\ 827$	93
15	504	31	$31 \cdot 504^{(790)} mod\ 827$	99
16	273	513	$513 \cdot 273^{(790)} mod\ 827$	103
17	108	18	$18 \cdot 108^{(790)} mod\ 827$	95
18	218	190	$190 \cdot 218^{(790)} mod\ 827$	104

b. Setelah mendapatkan plainteks dari proses dekripsi tahap pertama, plainteks tersebut didekripsi kembali menggunakan metode *Vigènere Cipher*. Proses dekripsi tahap kedua menggunakan perhitungan sebagai berikut [9]:

$$P_i = ((P_i - K_i - 32) mod\ 95) + 32$$

Sebelum melakukan proses dekripsi, langkah pertama dalam proses dekripsi metode *Vigènere Cipher* adalah menentukkan indeks karakter dari kunci publik $(p, \alpha, \beta) = (827, 37, 276)$. Indeks karakter dari kunci publik ditampilkan pada tabel:

Tabel 7. Indeks Karakter Kunci

Kunci	Indeks	Kunci	Indeks

8	56	,	44
2	50	2	50
7	55	7	55
,	44	6	54
3	51		
7	55		

c. Sehingga proses dekripsi tahap kedua adalah sebagai berikut:

Tabel 8. Proses Dekripsi Tahap Kedua

i	Cipherteks	Kunci	$D = ((C_i - K_i - 32) mod\ 95) + 32$	Plainteks
1	37	56	$((37 - 56 - 32) mod\ 95) + 32$	76
2	72	50	$((72 - 50 - 32) mod\ 95) + 32$	117
3	60	55	$((60 - 55 - 32) mod\ 95) + 32$	100
4	70	44	$((70 - 44 - 32) mod\ 95) + 32$	121
5	53	51	$((53 - 51 - 32) mod\ 95) + 32$	97
6	79	55	$((79 - 55 - 32) mod\ 95) + 32$	119
7	46	44	$((46 - 44 - 32) mod\ 95) + 32$	97
8	71	50	$((71 - 50 - 32) mod\ 95) + 32$	116
9	65	55	$((65 - 55 - 32) mod\ 95) + 32$	105
10	99	54	$((99 - 54 - 32) mod\ 95) + 32$	45
11	105	56	$((105 - 56 - 32) mod\ 95) + 32$	49
12	107	50	$((107 - 50 - 32) mod\ 95) + 32$	57
13	109	55	$((109 - 55 - 32) mod\ 95) + 32$	54
14	93	44	$((93 - 44 - 32) mod\ 95) + 32$	49
15	99	51	$((99 - 51 - 32) mod\ 95) + 32$	48
16	103	55	$((103 - 55 - 32) mod\ 95) + 32$	48
17	95	44	$((95 - 44 - 32) mod\ 95) + 32$	51
18	104	50	$((104 - 50 - 32) mod\ 95) + 32$	54

d. Langkah selanjutnya plainteks yang dihasilkan dari proses dekripsi tahap kedua dibuah menjadi karakter menggunakan tabel ASCII *printable*. Plainteksnya adalah

Tabel 9. Proses Pengubahan Indeks menjadi Karakter

Plainteks	Simbol	Plainteks	Simbol
76	L	45	-
117	u	49	1

100	d	57	9
121	y	54	6
97	a	49	1
119	w	48	0
97	a	48	0
116	t	51	3
105	i	54	6

KESIMPULAN

Proses Enkripsi kombinasi metode *Vigènere Cipher* dan ElGamal diawali dengan proses pembentukan kunci menggunakan Algoritma Elgamal. Kunci yang dibentuk adalah kunci publik($\boldsymbol{p}, \boldsymbol{\alpha}, \boldsymbol{\beta}$) dan kunci rahasia $\boldsymbol{d}$. Proses pembentukan kunci dipengaruhi beberapa komponen yang harus dipenuhi, yaitu bilangan prima aman besar $\boldsymbol{p}$ yang dihasilkan dari software Python, akar primitif $\boldsymbol{\alpha}$ dari bilangan prima $\boldsymbol{p}$, dan bilangan bulat $\boldsymbol{d}$ yang berasal dari tiga digit terakhir dari NIM. Untuk lebih memperkuat kunci publik dilakukan pengecekan keprimaan aman dan juga akar primitif. Proses enkripsi dilakukan sebanyak dua kali yaitu proses enkripsi menggunakan metode *Vigènere Cipher* dan ElGamal. Kekuatan dari proses enkripsi tergantung pada kunci publik dan perhitungan modulo yang digunakan. Terlebih lagi pada proses enkripsi dengan Algoritma ElGamal karena kekuatan keamanan Enkripsi dari ElGamal tergantung pada bilangan prima besar dan juga akar primitif dari bilangan prima tersebut. Pada enkripsi metode *Vigènere Cipher* cipherteks diperkuat dengan menggunakan perhitungan modulo ASCII *printable*. Perhitungan dari modulo ini dapat meningkatkan keamanan dari cipherteks karena perhitungan yang digunakan berbeda dengan perhitungan modulo *tabula recta* atau tabel ASCII keseluruhan.

Proses Dekripsi kombinasi metode *Vigènere Cipher* dan ElGamal diawali dengan melakukan proses dekripsi tahap pertama. Proses dekripsi tahap pertama dilakukan menggunakan Algoritma ElGamal. Pada proses ini kunci yang digunakan adalah kunci rahasia ($\boldsymbol{p}, \boldsymbol{d}$). Setelah proses tersebut dilanjutkan dengan proses dekripsi tahap kedua dengan menggunakan metode *Vigènere Cipher*. Perhitungan yang digunakan pada proses ini adalah menggunakan perhitungan modulo ASCII *printable*. Dan proses dekripsi kombinasi metode *Vigènere Cipher* dan ElGamal dapat mengembalikan atau memulihkan cipherteks menjadi pesan asli seperti semula.

DAFTAR PUSTAKA

[1] Munir, R. (2019). KRIPTOGRAFI (Edisi Kedua). Bandung: Informatika Bandung.

[2] Sadikin, R. (2012). Kriptografi untuk Keamanan jaringan. Yogyakarta: C.V ANDI OFFSET.

[3] ElGamal, T. (1985). *A Publik Key Cryptosystem and a Signature Scheme Based on Discrete Logaritms*. IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-31, NO.4

[4] Andrian, Y., (2014). Perbandingan Penggunaan Bilangan Prima Aman dan Tidak Aman pada Proses Pembentukan Kunci Algoritma ElGamal. *Citec Journal* Vol. 1, No. 3, 194-203.

[5] Ariska, B., & Endri, J. (2018). Rancangan Kriptografi Hybrid Kombinasi Metode *Vigenere Cipher* Dan Elgamal Pada Pengamanan Pesan Rahasia. Seminar Nasional Inovasi dan Aplikasi di Industri, 328-336.

[6] Fadilla, D. V. (2017). Implementasi Algoritma Elgamal Dan *Vigenere Cipher* Untuk Enkripsi Dan Dekripsi Data Citra Digital. Jurnal Universitas Teknologi Yogyakarta.

[7] Ummi, K. (2013). Analisis Penggunaan Bilangan Prima Aman Besar Pada Algoritma ElGamal. *Proceedings* Konferensi Nasional Sistem Informasi, 1-5.

[8] Basyiah, Syahputra. F., (2017). Perancangan Aplikasi Penyandian Pesan Teks Menggunakan *Vigenere Cipher* dan Algoritma ElGamal. http://ejournal.ust.ac.id/index.php/Jurnal_Means, 80-85.

[9] Putri, R. A., Santoso, K. A., & Kamsyakawumi, A. (2021). Pengkodean *Polyalphabetic* dengan Modifikasi Algoritma ElGamal-*Caesar Cipher*. Prosiding Seminar Nasional Matematika, 540-547.

[10] Ariyus, D. (2008). Pengantar Ilmu Kriptografi Teori, Analisis, dam Implementasi. Yogyakarta: C.V ANDI OFFSET.

[11] Stinson, D.R., (1995). *Cryptography Theory and Practice*. Florida: CRC Press, Inc.

[12] Ifanto, M. (2009). Metode Enkripsi dan Dekripsi Menggunakan Algoritma ElGamal. Jurnal Institut Teknologi Bandung.

[13] Irawan, D. M. (2017). Implementasi Kriptografi *Vigenere Cipher* dengan Php. Jurnal teknologi Informasi Volume 1, 11-21

[14] Yani, E. C. (2009). Analisis dampak Pemilihan Nilai Bilangan Prima pada Properti Algoritma ElGamal *p* terhadap Kekuatan Pengamanan Data. Jurnal Institut Teknologi Bandung.

[15] Ariyus, D. (2006). KRIPTOGRAFI (Edisi Pertama). Yogyakarta: Penerbit Graha Ilmu.