Jurnal Riset Mahasiswa Matematika
Volume 1(5) (2022), Pages 230-235
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Penggabungan Algoritma Hill Cipher dan ElGamal untuk Mengamankan Pesan teks

Siti Nur Fadlilah, Turmudi, Muhammad Khudzaifah

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

dilafadilah84435@gmail.com, turmudi_msi@mat.uin-malang.ac.id, khudzaifah@uin-malang.ac.id

Abstrak

Hill Cipher merupakan salah satu algoritma kriptografi kunci simetris yang menggunakan matriks *invertible* dengan *ordo* $n \times n$ sebagai kunci untuk melakukan enkripsi dan dekripsi pada *plaintext*. Sedangkan *ElGamal* merupakan salah satu algoritma kriptografi kunci asimetris yang memanfaatkan kerumitan logaritma diskrit pada proses enkripsi dan dekripsi. Pada penelitian ini, penulis tertarik menggabungkan algoritma *Hill Cipher* dan *ElGamal* untuk mengamankan pesan teks. Peneliti menggunakan matriks 3×3 sebagai kunci simetris dan mengonversikan *plaintext* pada tabel ASCII 256. Kemudian melakukan enkripsi menggunakan algoritma *Hill Cipher* yang menghasilkan *ciphertext* dari pesan dan algoritma *ElGamal* menghasilkan *ciphertext* dari kunci simetris. Pada proses dekripsi menggunakan algoritma *ElGamal* untuk mengetahui kunci simetris yang akan digunakan sebagai kunci pada proses dekripsi dengan algoritma *Hill Cipher* sehingga diperoleh *plaintext* semula. Maka diperoleh hasil bahwa penggabungan algoritma *Hill Cipher* dan *ElGamal* untuk mengamankan pesan teks dapat dilakukan dengan baik.

Kata Kunci: Dekripsi; Enkripsi; *ElGamal; Hill Cipher*.

Abstract

Hill Cipher is a one of the symmetric key cryptography algorithms that using an invertible matrix with an order $n \times n$ as a key to encrypt and decrypt plaintext. Meanwhile, ElGamal is other asymmetric key cryptography algorithm that use the complexity of discrete logarithms in the encryption and decryption process. In this study, the authors are interest in combine the Hill Cipher and ElGamal algorithms to secure text messages. The author uses the matrix as a symmetric key and converts the plaintext in the table of ASCII 256. Then encrypt using the Hill Cipher algorithm which results the ciphertext from messages and ElGamal algorithm results the ciphertext of the symmetric key. In processing decryption using the ElGamal algorithm to determine the symmetric key that will be used as a key in the decryption process with the Hill Cipher algorithm so that the original plaintext is obtained. Then the results obtained are that the combination of the Hill Cipher and ElGamal algorithms to secure text messages can be done it well.

Keywords: Decryption; Encryption; ElGamal; Hill Cipher

PENDAHULUAN

Aspek penting dalam sistem informasi yaitu keamanan dan kerahasiaan pesan. semakin berkembangnya teknologi informasi mengakibatkan tingkat serangan kriptanalis semakin tinggi sehingga pencurian informasi sering terjadi. Cara untuk mengurangi serangan kriptanalis yaitu dengan menggunakan metode penyandian yang dikenal dengan kriptografi [1]. Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Keamanan pesan diperoleh dengan melakukan penyandian menjadi pesan yang tidak memiliki makna. Pesan asli disebut sebagai *plaintext* sedangkan pesan baru yang berbentuk kode disebut *ciphertext*. Proses mengubah *plaintext*

Submitted: 20 Desember 2021 Reviewed: 26 Mei 2022 Accepted: 26 Juni 2022
Doi: http://dx.doi.org/10.18860/jrmm.v1i5.14496

menjadi *ciphertext* disebut enkripsi sedangkan dekripsi merupakan proses mengubah *ciphertext* menjadi *plaintext* [2].

Pada tahun 1929 Laster S. Hill melakukan proses penyandian menggunakan perkalian matriks dengan pendekatan aljabar [3]. Algoritma *Hill Cipher* mampu menghadapi serangan *Ciphertext-Only Attack* (COA) namun COA dapat dipecahkan dengan *Chinese Remainder Theorem* sehingga keamanan pada algoritma *Hill Cipher* harus ditingkatkan. Kelemahan utama algoritma *Hill Cipher* adalah menggunakan persamaan linier dengan matriks sebagai operasi substitusi. Apabila penyerang mampu mengumpulkan pasangan teks asli dan teks sandi yang menggunakan kunci yang sama, penyerang dapat menemukan kunci *Hill Cipher* dengan menyelesaikan sistem persamaan linier. Algoritma *Hill Cipher* menggunakan kunci yang sama ketika melakukan proses enkripsi dan dekripsi, sehingga algoritma *Hill Cipher* merupakan algoritma kriptografi dengan kunci simetris. Kunci yang digunakan berbentuk matriks persegi yang memiliki invers [4].

Pada tahun 1985, Taher *ElGamal* memperkenalkan algoritma *ElGamal* dengan tiga proses yang dilakukan yaitu, pembentukan kunci, enkripsi *plaintext* dan dekripsi *ciphertext*. Algoritma ini didasarkan atas masalah logaritma diskrit. Algoritma *ElGamal* merupakan salah satu algoritma kunci asimetris sehingga memiliki kunci yang berbeda untuk melakukan enkripsi dan dekripsi yaitu, kunci publik yang dibentuk oleh pengirim dan kunci privat yang dibentuk oleh penerima sehingga pengirim tidak mengetahui kunci privat [5].

Suci Ramadani mengombinasikan algoritma *Hill Cipher* dan *ElGamal* diterapkan pada citra. Keamanan citra menggunakan algoritma *Hill Cipher* dan *ElGamal* berhasil di enkripsi dan di dekripsi dengan baik. Waktu yang diperlukan untuk melakukan dekripsi lebih cepat daripada melakukan proses enkripsinya [6].

METODE

Langkah-Langkah Penelitian

Langkah-langkah yang dilakukan untuk mengetahui proses enkripsi dan dekripsi menggunakan algoritma *Hill Cipher* dan *ElGamal* untuk mengamankan pesan teks adalah:

1. Pembentukan kunci *Hill Cipher* dengan memilih matriks *invertible* $K_{3\times3}$.
2. Pembentukan kunci algoritma *ElGamal*.
   a) Memilih bilangan prima p.
   b) Menentukan α yang merupakan akar primitif p.
   c) Pilih sembarang bilangan bulat d dengan $1 \leq d \leq p-2$.
   d) Menghitung $\beta = \alpha^d mod\ p$.
   e) Menentukan kunci publik (p, α, β) dan kunci privat d.
   f) Pilih r yang merupakan sembarang elemen matriks dengan $r \in \{0,1,2,\cdots, p-2\}$.
3. Proses enkripsi menggunakan algoritma *Hill Cipher.*
   a) Menentukan *plaintext* dan mengonversikan pada tabel ASCII 256.
   b) Mengubah *plaintext* menjadi blok-blok sesuai dengan *ordo* matriks kunci $K_{3\times3}$.
   c) Hitung menggunakan rumus algoritma *Hill Cipher* $C = K \cdot P\ mod\ N$.
4. Proses enkripsi menggunakan algoritma *ElGamal*.
   a) Ubah elemen kunci $K_{3\times3}$ menjadi *plaintext* (P).
   b) Gunakan kunci publik untuk menghitung $a = \alpha^r\ mod\ p$ dan $b = P \cdot \beta^r\ mod\ p$.
5. Proses dekripsi menggunakan algoritma *ElGamal*.
   a) Gunakan kunci privat.
   b) Hitung $P = b \times (a^x)^{-1}$ dengan menentukan $(a^x)^{-1} = a^{P-1-d}$.
6. Proses dekripsi menggunakan algoritma *Hill Cipher* .
   a) Tentukan invers matriks $K_{3\times3}$.
   b) Hitung $P = \overline{K} \cdot C\ mod\ N$

HASIL DAN PEMBAHASAN

1. Pembentukan Kunci Algoritma *Hill Cipher* dan *ElGamal*

a. Pembentukan Kunci Algoritma *Hill Cipher*

Pilih kunci $K = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}$

Tentukan $det\ K \neq 0$ dengan menghitung minor kofaktor K,

$M_{11} = 13 \qquad M_{21} = 5 \qquad M_{31} = 2$

$det\ K = 1 \cdot 13 - 2 \cdot 5 + 3 \cdot 2 = 13 - 10 + 6 = 9$

Diketahui $det\ K = 9$, maka matriks K *invertible*

b. Pembentukan Kunci Algoritma *ElGamal*

Memilih bilangan prima $p = 241$. Pilih akar primitif pada $(\mathbb{Z}_{241}^{*}, \times)$, misal dipilih $\alpha = 11$. Memilih sembarang bilangan bulat $d = 197$ yang memenuhi $1 \leq d \leq p - 2$. Dari perhitungan menggunakan $\beta = \alpha^{d} mod\ p$ sehingga diperoleh $\beta = 63$. Diperoleh kunci publik $(p, \alpha, \beta) = (241, 11, 63)$ dan kunci privat $d = 197$. Menentukan $r = \begin{bmatrix} 236 & 174 & 234 \\ 182 & 222 & 155 \\ 224 & 97 & 132 \end{bmatrix}$.

2. Enkripsi Menggunakan Algoritma *Hill Cipher* dan *ElGamal*

a. Pembentukan *Plaintext*

Plaintext yang digunakan pada penelitian ini adalah **Saya Mahasiswa Matematika 2017** dan konversikan pada tabel ASCII 256 sebagai berikut,

Tabel 1. Konversi *Plaintext* pada Kode ASCII 256

S	a	y	a	spasi	M	a	H	a	s
83	97	121	97	32	77	97	104	97	115
i	s	w	a	spasi	M	a	T	e	m
105	115	119	97	32	77	97	116	101	109
a	t	i	k	a	spasi	2	0	1	7
97	116	105	107	97	32	50	48	49	55

Ubah *plaintext* menjadi blok-blok sesuai dengan *ordo* kunci $K_{3\times3}$,

$p_1 = \begin{bmatrix} 83 \\ 97 \\ 121 \end{bmatrix}\ p_2 = \begin{bmatrix} 97 \\ 32 \\ 77 \end{bmatrix}\ p_3 = \begin{bmatrix} 97 \\ 104 \\ 97 \end{bmatrix}\ p_4 = \begin{bmatrix} 115 \\ 105 \\ 115 \end{bmatrix}\ p_5 = \begin{bmatrix} 119 \\ 97 \\ 32 \end{bmatrix}$

$p_6 = \begin{bmatrix} 77 \\ 97 \\ 116 \end{bmatrix}\ p_7 = \begin{bmatrix} 101 \\ 109 \\ 97 \end{bmatrix}\ p_8 = \begin{bmatrix} 115 \\ 105 \\ 107 \end{bmatrix}\ p_9 = \begin{bmatrix} 97 \\ 32 \\ 50 \end{bmatrix}\ p_{10} = \begin{bmatrix} 48 \\ 49 \\ 55 \end{bmatrix}$

b. Proses Enkripsi Menggunakan Algoritma *Hill Cipher* pada Pesan

Enkripsi dilakukan dengan rumus $C = K \cdot P\ mod\ N$ sebagai berikut,

$$c_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 83 \\ 97 \\ 121 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 83 + 194 + 363 \\ 166 + 776 + 847 \\ 83 + 485 + 726 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 640 \\ 1789 \\ 1294 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 128 \\ 253 \\ 14 \end{bmatrix} = \begin{bmatrix} Ç \\ ² \\ SO \end{bmatrix}$$

$$c_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 97 \\ 32 \\ 77 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 97 + 64 + 231 \\ 194 + 256 + 539 \\ 97 + 160 + 462 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 392 \\ 989 \\ 719 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 136 \\ 221 \\ 207 \end{bmatrix} = \begin{bmatrix} ê \\ ¦ \\ ¤ \end{bmatrix}$$

Lakukan perhitungan hingga p_{10} hingga diperoleh *ciphertext* sebagai berikut,

$c_1 = \begin{bmatrix} Ç \\ ² \\ SO \end{bmatrix}$ $c_2 = \begin{bmatrix} ê \\ ¦ \\ ¤ \end{bmatrix}$ $c_3 = \begin{bmatrix} T \\ ® \\ » \end{bmatrix}$ $c_4 = \begin{bmatrix} × \\ S \\ 2 \end{bmatrix}$ $c_5 = \begin{bmatrix} Ö \\ Í \\ FS \end{bmatrix}$

$c_6 = \begin{bmatrix} K \\ ┼ \\ Û \end{bmatrix}$ $c_7 = \begin{bmatrix} B \\ ┘ \\ ├ \end{bmatrix}$ $c_8 = \begin{bmatrix} å \\ ESC \\ STX \end{bmatrix}$ $c_9 = \begin{bmatrix} 7 \\ Space \\ — \end{bmatrix}$ $c_{10} = \begin{bmatrix} 7 \\ I \\ 0 \end{bmatrix}$

c. Enkripsi Menggunakan Algoritma *ElGamal* pada Kunci Simetris *K*

Kemudian proses enkripsi dengan algoritma *ElGamal* menggunakan kunci publik dan r untuk menghitung $a = \alpha^r \ mod \ p$ dan $b = P \cdot \beta^r \ mod \ p$,

$a = \alpha^r mod\ p$
$= 11^{236} mod\ 241$
$= 4$

$b = P \times \beta^r mod\ p$
$= 1 \times 63^{236} mod\ 241$
$= 60$

$a = \alpha^r mod\ p$
$= 11^{174} mod\ 241$
$= 30$

$b = p \times \beta^r mod\ p$
$= 2 \times (63^6)^{29} mod\ 241$
$= 181$

Hasil enkripsi kunci K dapat di lihat pada tabel 2,

Tabel 2. Hasil Enkripsi Kunci

Key	***a***	***b***
[1,1]	4	60
[1,2]	30	181
[1,3]	8	217
[2,1]	32	4
[2,2]	30	1
[2,3]	38	100
[3,1]	15	225
[3,2]	11	74
[3,3]	64	143

3. Dekripsi menggunakan algoritma *ElGamal* dan *Hill Cipher*

a. Dekripsi Menggunakan Algoritma *ElGamal* pada Kunci Simetris *K*

Dekripsi Menggunakan rumus algoritma *ElGamal* $P_{[1,1]} = b \times (a^x)^{-1} \ mod \ p$ dengan menentukan terlebih dahulu $(a^x)^{-1} = a^{p-1-d} \ mod \ p$ sebagai berikut,

$c_{[1,1]} = (a, b) = (4{,}60)$
$(a^x)^{-1} = a^{p-1-d} \ mod \ p$
$= 4^{241-1-197} mod\ 241$
$= 237$

$P_{[1,1]} = b \times (a^x)^{-1} \ mod \ p$
$= 60 \times 237 \ mod\ 241$
$= 14220 \ mod\ 241$
$= 1$

$c_{[1,2]} = (a, b) = (30{,}181)$
$(a^x)^{-1} = a^{p-1-d} \ mod \ p$
$= 30^{241-1-197} mod\ 241$
$= 8$

$P_{[1,2]} = b \times (a^x)^{-1} \ mod \ p$
$= 181 \times 8 \ mod\ 241$
$= 1448 \ mod\ 241$
$= 2$

Proses dekripsi dilakukan hingga $P_{[3,3]}$, sehingga dapat dilihat hasil dekripsi pada tabel sebagai berikut,

Tabel 3. Hasil Dekripsi Kunci

Key	***Plaintext***
[1,1]	1
[1,2]	2
[1,3]	3
[2,1]	2

[2,2]	8
[2,3]	7
[3,1]	1
[3,2]	5
[3,3]	6

b. Dekripsi Menggunakan Algoritma *Hill Cipher* pada Pesan

Kemudian proses dekripsi menggunakan algoritma *Hill Cipher* dengan rumus $P = \overline{K} \cdot C \ mod \ N$ sehingga perlu menentukan $\overline{K}$ modulo 256 dengan rumus $\overline{K} = \bar{\Delta} \cdot adj(K)$. Diketahui $det\ K = 9$ sehingga untuk menentukan $\bar{\Delta}$ merupakan invers dari 9 mod 256 yaitu,

$$\begin{aligned} 9 \ mod \ 256 = 9 \cdot x &\equiv 1 \ mod \ 256 \\ 9 \cdot x &\equiv 256y + 1 \\ 9 \cdot x - 256y &\equiv 1 \ mod \ 256 \\ 9 \cdot 57 - 256 \cdot 1 &\equiv 1 \ mod \ 256 \\ 513 - 256 &\equiv 1 \ mod \ 256 \\ 257 &\equiv 1 \ mod \ 256 \end{aligned}$$

Kemudian menentukan $adj(K)$ sebagai berikut,

Diketahui $K = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}$

$$\begin{array}{lll} M_{11} = 13 & M_{12} = -3 & M_{13} = -10 \\ M_{21} = 5 & M_{22} = 3 & M_{23} = 1 \\ M_{31} = 2 & M_{32} = 3 & M_{33} = 4 \end{array}$$

Diperoleh $minor\ K = \begin{bmatrix} 13 & 5 & 2 \\ -3 & 3 & 3 \\ -10 & 1 & 4 \end{bmatrix}$ maka $kof\ K = \begin{bmatrix} 13 & -5 & 2 \\ 3 & 3 & -3 \\ -10 & -1 & 4 \end{bmatrix}$ sehingga diperoleh $adj\ K = \begin{bmatrix} 13 & 3 & -10 \\ -5 & 3 & -1 \\ 2 & -3 & 4 \end{bmatrix}$. Menentukan $\overline{K}$ modulo 256 adalah,

$$\begin{aligned} \overline{K} &= \bar{\Delta} \cdot (adj\ K) \ mod \ 256 \\ &= 57 \cdot \begin{bmatrix} 13 & 3 & -10 \\ -5 & 3 & -1 \\ 2 & -3 & 4 \end{bmatrix} mod \ 256 \\ &= \begin{bmatrix} 741 & 171 & -570 \\ -285 & 171 & -57 \\ 114 & -171 & 228 \end{bmatrix} mod \ 256 \\ &= \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \end{aligned}$$

Proses dekripsi dilakukan menggunakan rumus dekripsi algoritma *Hill Cipher* $P = \overline{K} \cdot C \ mod \ N$ sebagai berikut,

$$\begin{aligned} p_1 &= \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 128 \\ 253 \\ 14 \end{bmatrix} \\ &= \begin{bmatrix} 29312 + 43263 + 2772 \\ 29056 + 43263 + 2786 \\ 14592 + 21505 + 3192 \end{bmatrix} \\ &= \begin{bmatrix} 75347 \\ 75105 \\ 39289 \end{bmatrix} mod \ 256 \\ &= \begin{bmatrix} 83 \\ 97 \\ 121 \end{bmatrix} = \begin{bmatrix} S \\ a \\ y \end{bmatrix} \end{aligned}$$

$$\begin{aligned} p_2 &= \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 136 \\ 221 \\ 207 \end{bmatrix} \\ &= \begin{bmatrix} 31144 + 37791 + 40986 \\ 30872 + 37791 + 41193 \\ 15504 + 18785 + 47196 \end{bmatrix} \\ &= \begin{bmatrix} 109921 \\ 109856 \\ 81485 \end{bmatrix} mod \ 256 \\ &= \begin{bmatrix} 97 \\ 32 \\ 77 \end{bmatrix} = \begin{bmatrix} a \\ spasi \\ M \end{bmatrix} \end{aligned}$$

Diperoleh *plaintext* semula sebagai berikut,

$$p_1 = \begin{bmatrix} S \\ a \\ y \end{bmatrix} p_2 = \begin{bmatrix} a \\ spasi \\ M \end{bmatrix} p_3 = \begin{bmatrix} a \\ h \\ a \end{bmatrix} p_4 = \begin{bmatrix} s \\ i \\ s \end{bmatrix} p_5 = \begin{bmatrix} w \\ a \\ spasi \end{bmatrix}$$

$$p_6 = \begin{bmatrix} M \\ a \\ t \end{bmatrix} p_7 = \begin{bmatrix} e \\ m \\ a \end{bmatrix} p_8 = \begin{bmatrix} t \\ i \\ k \end{bmatrix} p_9 = \begin{bmatrix} a \\ spasi \\ 2 \end{bmatrix} p_{10} = \begin{bmatrix} 0 \\ 1 \\ 7 \end{bmatrix}$$

Berdasarkan hasil dekripsi yang kedua menggunakan algoritma *Hill Cipher* diperoleh *plaintext* semula yaitu **Saya Mahasiswa Matematika 2017**.

KESIMPULAN

Berdasarkan penelitian di atas dapat disimpulkan bahwa, penggabungan algoritma *Hill Cipher* dan *ElGamal* pada pesan teks dapat dilakukan menggunakan perhitungan matematika manual. Pesan yang dikirimkan dapat di enkripsi dan dekripsi dengan baik. Sehingga pesan yang dikirimkan sesuai dengan pesan yang diterima yang berarti bahwa pesan terhindar dari serangan kriptanalis.

DAFTAR PUSTAKA

[1] Jamaludin, "Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem," *Sinkron,* vol. II, pp. 86-93, April 2018.

[2] R. Munir, Matematika Diskrit, Edisi 3 ed., Bandung: Informatika Bandung, 2010, p. 205.

[3] L. S. Hill, "Cryptography in An Algebraic Alphabet," *The American Mathematical Monthly,* pp. 306 - 312, 1929.

[4] D. Ariyus, Pengantar Ilmu Komputer Teori Analisis dan Implementasi, F. Suryantoro, Ed., Yogyakarta: C.V ANDI OFFSET, 2008.

[5] R. Sadikin, Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java, T. A. Prabawati, Penyunt., Yogyakarta: C.V ANDI OFFSET, 2012, p. 9.

[6] S. Ramadani, "HYBIRD CRYPTOSYSTEM ALGORITMA HILL CIPHER DAN ALGORITMA," *METHOMIKA,* vol. IV, pp. 1-9, April 2020.

[7] S. S. K. Ahmadi, "Ciphertext-only attack on d x d Hill in O(d13^d)," pp. 1-16, 2016.