MATHEMATICAL SCIENCES AND APPLICATIONS JOURNAL

Volume 4, Number 1 | ISSN: 2986-4180

https://online-journal.unja.ac.id/msa

Article

Aplikasi Modifikasi Algoritma Vigenere *Cipher* dan Hill *Cipher* Menggunakan Konversi Suhu

Aurillya Queency, Sisilia Sylviani*

Departemen Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Padjadjaran, Sumedang 45363, Indonesia

*Corresponding author e-mail: sisilia.sylviani@unpad.ac.id

Article Info
Received October 2023
Accepted October 2023
Published October 2023

Keyword:
Cryptography
Decryption
Encryption
Hill Cipher
Temperature conversion
Vigenere Cipher

Abstract

Cryptography is a method used to maintain the confidentiality of messages and data. Modifications or combinations of algorithms can be made to make the process of cracking secret messages more difficult than just one algorithm. This research aims to apply a combination of modified Vigenere Cipher algorithm, modified Hill Cipher algorithm, and temperature conversion equations to maintain a message's confidentiality. By determining one plaintext and the required keys, the encryption and decryption process uses a modified Vigenere Cipher algorithm, a modified Hill Cipher algorithm, and all temperature conversion equations. The results obtained in the encryption process of one plaintext are 12 different ciphertexts according to the temperature conversion equation used. Moreover, the results obtained in the decryption process of 12 different ciphertexts are the original plaintext.

1. Pendahuluan

Pada era digital, komunikasi menjadi semakin mudah karena beragamnya media komunikasi yang sejalan dengan perkembangan teknologi digital. Namun, di sisi lain, banyak jaringan yang tidak dapat menjamin keamanan pesan yang dikirim melalui jaringan tersebut. Oleh karena itu, dibutuhkan teknik untuk mengamankan pesan-pesan tersebut, khususnya pesan-pesan yang bersifat rahasia bagi pengirim dan penerimanya agar tidak dapat dibaca oleh pihak lain.

Terdapat berbagai macam teknik yang digunakan untuk mengamankan suatu pesan. Terdapat dua teknik pengamanan pesan yang saat ini sedang banyak digunakan, yaitu steganografi dan kriptografi. Steganografi merupakan ilmu dengan teknik-teknik tertentu yang bertujuan untuk menyembunyikan suatu pesan agar orang lain selain pengirim dan penerima tidak dapat mengetahui keberadaan pesan tersebut [1]. Sedangkan, kriptografi merupakan ilmu yang bertujuan untuk menjaga keamanan pesan dengan mengubah pesan tersebut menjadi kode-kode yang hanya dipahami oleh pengirim dan penerima [2]. Kriptografi mentransformasikan sebuah pesan (plainteks) ke dalam bentuk sandi (cipherteks) yang berguna dalam menjaga kerahasiaan pesan. Saat pesan sampai kepada penerima, pesan tersebut ditransformasikan kembali ke dalam bentuk plainteks semula [3]. Proses transformasi dari plainteks menjadi cipherteks disebut sebagai enkripsi atau *encryption*, sedangkan proses transformasi dari cipherteks menjadi plainteks semula disebut sebagai dekripsi atau *decryption* [4]. Pada proses enkripsi dan dekripsi dibutuhkan kunci tertentu sesuai dengan algoritma atau *cipher* yang digunakan. Algoritma merupakan fungsi-fungsi matematika yang diperlukan dalam proses enkripsi dan dekripsi [2], sedangkan kunci merupakan sederatan bit yang digunakan saat proses enkripsi dan dekripsi [3].

Algoritma dalam kriptografi sangatlah banyak. Beberapa di antaranya adalah algoritma Vigenere *Cipher* dan Hill *Cipher*. Algoritma Vigenere *Cipher* merupakan algoritma yang mentransformasikan plainteks berupa huruf dengan menggeser huruf tersebut sejauh nilai kunci pada deret alfabet [5]. Algoritma Vigenere *Cipher* adalah pengembangan dari sandi Caesar, yaitu setiap huruf pada plainteks ditransformasikan menjadi huruf lain yang memiliki perbedaan yang bersifat tetap pada deret

https://doi.org/10.22437/msa.v4i1.28858

alfabet. Penelitian terkait algoritma Vigenere *Cipher* sudah banyak dilakukan, seperti analisis perbandingan antara algoritma Vigenere *Cipher* dengan One Time Pad [6], penggunaan algoritma Vigenere *Cipher* pada *software* PHP [5] dan bahasa pemrograman Python [7], serta modifikasi algoritma Vigenere *Cipher* dengan menggunakan tabel Vigenere berukuran 95×95 [8]. Selain itu, algoritma Hill *Cipher* merupakan algoritma yang menggunakan aritmatika modulo dan perkalian matriks dengan matriks persegi sebagai kunci pada proses enkripsi dan dekripsinya [9]. Penelitian-penelitian terkait algoritma Hill *Cipher* di antaranya adalah modifikasi algoritma Hill *Cipher* dengan *convert between base* [10], matriks modular [11], dua matriks kunci dan 94 karakter ASCII [12], serta matriks kunci ortogonal dan TSLRS [13]. Jika kedua algoritma tersebut dikombinasikan, maka pesan rahasia akan lebih sulit untuk diketahui oleh pihak lain dibandingkan dengan hanya menggunakan satu algoritma. Penelitian yang menerapkan kombinasi dua algoritma salah satunya adalah kombinasi algoritma Vigenere *Cipher* dan Hill *Cipher* [9, 14–16].

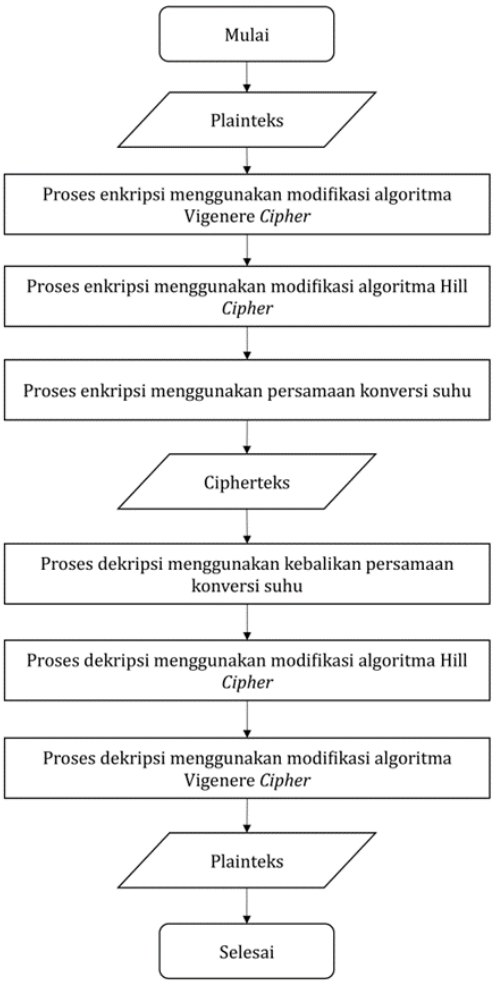
Pada penelitian [16] dibahas mengenai penerapan kombinasi algoritma Vigenere *Cipher*, Hill *Cipher*, dan persamaan konversi suhu sebagai pengaman sebuah pesan. Teknik pengamanan sebuah pesan pada penelitian ini juga menggunakan kombinasi dari algoritma-algoritma tersebut karena algoritma Vigenere *Cipher* dan Hill *Cipher* memiliki kemungkinan kunci yang sangat banyak serta terdapat tiga persamaan konversi suhu yang dapat menjadi kunci dekripsi suatu pesan rahasia sehingga pesan rahasia tersebut sangat sulit untuk dipecahkan oleh pihak lain. Berbeda dari penelitian [16], pada penelitian ini digunakan 62 karakter, matriks kunci berukuran 3×3 untuk algoritma Hill *Cipher*, dan persamaan konversi suhu untuk mentransformasikan satu plainteks menjadi 12 cipherteks yang berbeda.

2. Metode Penelitian

Metode yang digunakan pada penelitian ini adalah studi literatur terkait kriptografi, algoritma Vigenere *Cipher*, dan algoritma Hill *Cipher*. Penelitian ini dibagi menjadi dua bagian, yaitu proses enkripsi dan proses dekripsi. Diagram alir penelitian ini dapat dilihat pada Gambar 1.

2.1. Proses Enkripsi

Pada proses enkripsi, langkah pertama yang dilakukan adalah mendefinisikan plainteks berupa huruf dan/atau angka. Selanjutnya, plainteks tersebut diubah ke dalam



Gambar 1. Diagram alir penelitian

bentuk numerik. Daftar karakter dan nilai yang digunakan pada penelitian ini dapat dilihat pada Tabel 1. Kemudian, digunakan modifikasi algoritma Vigenere *Cipher* dengan menggunakan sebuah kata kunci untuk memperoleh cipherteks pertama. Modifikasi tersebut adalah penambahan karakter dari 26 karakter alfabet menjadi 62 karakter gabungan antara alfabet dan angka. Secara matematis, enkripsi dengan menggunakan algoritma Vigenere *Cipher* yang telah dimodifikasi dapat dinyatakan sebagai

$$C_i^1 = (P_i + K_i) \bmod 61.$$

Keterangan:
C_i^1 : Nilai karakter cipherteks pertama urutan ke-i
P_i : Nilai karakter plainteks ke-i
K_i : Nilai karakter kunci ke-i

Selanjutnya, cipherteks diubah menjadi matriks 3×1 dan digunakan algoritma Hill *Cipher* yang telah dimodifikasi. Pada modifikasi Hill *Cipher*, digunakan matriks kunci berukuran 3×3.

Tabel 1. Daftar karakter dan nilainya

Karakter	Nilai	Karakter	Nilai	Karakter	Nilai	Karakter	Nilai
A	0	Q	16	g	32	w	48
B	1	R	17	h	33	x	49
C	2	S	18	i	34	y	50
D	3	T	19	j	35	z	51
E	4	U	20	k	36	0	52
F	5	V	21	l	37	1	53
G	6	W	22	m	38	2	54
H	7	X	23	n	39	3	55
I	8	Y	24	o	40	4	56
J	9	Z	25	p	41	5	57
K	10	a	26	q	42	6	58
L	11	b	27	r	43	7	59
M	12	c	28	s	44	8	60
N	13	d	29	t	45	9	61
O	14	e	30	u	46		
P	15	f	31	v	47		

Secara matematis, proses enkripsi dengan modifikasi Hill *Cipher* dapat dinyatakan sebagai:

$$\boldsymbol{C}_i^2 = \boldsymbol{K} \cdot \boldsymbol{C}_i^1 \bmod 61.$$

Keterangan:
$\boldsymbol{C}_i^1$: Matriks cipherteks pertama urutan ke-i
$\boldsymbol{C}_i^2$: Matriks cipherteks kedua urutan ke-i
$\boldsymbol{K}$: Matriks kunci

Kemudian, cipherteks kedua dikonversi menggunakan persamaan konversi suhu yang dinyatakan sebagai berikut:

a. Konversi celcius ke fahrenheit

$$C_i^3 = \frac{9}{5} C_i^2 + 32.$$

b. Konversi celcius ke kelvin

$$C_i^3 = C_i^2 + 273.$$

c. Konversi celcius ke reamur

$$C_i^3 = \frac{4}{5} C_i^2.$$

Keterangan:
C_i^2 : Nilai karakter cipherteks kedua urutan ke-i
C_i^3 : Nilai karakter cipherteks ketiga urutan ke-i

Persamaan konversi suhu lainnya dapat diturunkan dari persamaan konversi suhu yang sudah ada. Kemudian, perhitungan nilai karakter cipherteks ketiga dibulatkan menjadi maksimal dua digit desimal.

2.2. Proses Dekripsi

Pada proses dekripsi, langkah pertama adalah mendefinisikan cipherteks. Kemudian, cipherteks tersebut didekripsi menggunakan kebalikan dari persamaan konversi suhu yang telah ditentukan sehingga diperoleh plainteks pertama. Selanjutnya, plainteks pertama didekripsi menggunakan algoritma Hill *Cipher* yang telah dimodifikasi untuk memperoleh plainteks kedua, yaitu menggunakan invers matriks kunci berukuran 3×3 dan plainteks pertama diubah menjadi matriks 3×1.

Secara matematis, proses dekripsi dengan modifikasi Hill *Cipher* dapat dinyatakan sebagai

$$\boldsymbol{P}_i^2 = \boldsymbol{K}^{-1} \cdot \boldsymbol{P}_i^1 \bmod 61.$$

Keterangan:
$\boldsymbol{P}_i^1$: Matriks plainteks pertama urutan ke-i
$\boldsymbol{P}_i^2$: Matriks plainteks kedua urutan ke-i
$\boldsymbol{K}^{-1}$: Invers matriks kunci

Setelah itu, plainteks kedua didekripsi dengan menggunakan modifikasi algoritma Vigenere *Cipher* dengan menggunakan persamaan

$$P_i^3 = (P_i^2 - K_i) \bmod 61.$$

Keterangan:
P_i^2 : Nilai karakter plainteks kedua urutan ke-i
P_i^3 : Nilai karakter plainteks ketiga urutan ke-i
K_i : Nilai karakter kunci ke-i

Hasil yang diperoleh merupakan plainteks semula.

3. Hasil dan Diskusi

Pada penelitian ini dibahas proses enkripsi dari satu plainteks menjadi 12 cipherteks berbeda dengan menggunakan modifikasi algoritma Vigenere *Cipher*, modifikasi algoritma Hill *Cipher*, dan persamaan konversi suhu. Kemudian, pada proses dekripsi, 12 cipherteks tersebut didekripsikan kembali menjadi satu plainteks semula menggunakan algoritma-algoritma dengan kunci dan persamaan yang sebelumnya digunakan pada proses enkripsi. Berikut adalah hasil dan pembahasan dari penelitian ini.

3.1. Proses Enkripsi

Plainteks yang digunakan pada penelitian ini adalah "TEORI bilangan 01" yang berkorespondensi dengan nilai 19, 4, 14, 17, 8, 27, 34, 37, 26, 39, 32, 26, 39, 52, 53. Dengan menggunakan modifikasi algoritma Vigenere *Cipher* dan kata kunci "KONVERSI" yang berkorespondensi dengan nilai 10, 14, 13, 21, 4, 17, 18, 8, diperoleh hasil enkripsi pada Tabel 2.

Tabel 2. Hasil enkripsi menggunakan modifikasi algoritma Vigenere *Cipher*

i	P_i	C_i^1
1	19	29
2	4	18
3	14	27
4	17	38
5	8	12
6	27	44
7	34	52
8	37	45
9	26	36
10	39	53
11	32	45
12	26	47
13	39	43
14	52	8
15	53	10

Berdasarkan hasil pada Tabel 2, diperoleh cipherteks pertama yang berkorespondensi dengan nilai 29, 18, 27, 38, 12, 44, 52, 45, 36, 53, 45, 47, 43, 8, 10. Selanjutnya, digunakan modifikasi algoritma Hill *Cipher* untuk memperoleh cipherteks kedua. Matriks kunci yang digunakan pada algoritma Hill *Cipher* adalah matriks *invertible* atau matriks yang memiliki invers. Pada penelitian ini, digunakan matriks kunci *invertible* dengan entri sembarang berukuran 3×3 yang dinyatakan sebagai:

$$K = \begin{pmatrix} 7 & 5 & 9 \\ 1 & 4 & 3 \\ 2 & 3 & 5 \end{pmatrix}.$$

Dengan menggunakan modifikasi algoritma Hill *Cipher* diperoleh hasil sebagai berikut:

$$C_1^2 = \begin{pmatrix} 7 & 5 & 9 \\ 1 & 4 & 3 \\ 2 & 3 & 5 \end{pmatrix} \begin{pmatrix} 29 \\ 18 \\ 27 \end{pmatrix} \bmod 61 = \begin{pmatrix} 31 \\ 54 \\ 23 \end{pmatrix},$$

$$C_2^2 = \begin{pmatrix} 7 & 5 & 9 \\ 1 & 4 & 3 \\ 2 & 3 & 5 \end{pmatrix} \begin{pmatrix} 38 \\ 12 \\ 44 \end{pmatrix} \bmod 61 = \begin{pmatrix} 0 \\ 4 \\ 49 \end{pmatrix},$$

$$C_3^2 = \begin{pmatrix} 7 & 5 & 9 \\ 1 & 4 & 3 \\ 2 & 3 & 5 \end{pmatrix} \begin{pmatrix} 52 \\ 45 \\ 36 \end{pmatrix} \bmod 61 = \begin{pmatrix} 54 \\ 60 \\ 51 \end{pmatrix},$$

$$C_4^2 = \begin{pmatrix} 7 & 5 & 9 \\ 1 & 4 & 3 \\ 2 & 3 & 5 \end{pmatrix} \begin{pmatrix} 53 \\ 45 \\ 47 \end{pmatrix} \bmod 61 = \begin{pmatrix} 22 \\ 37 \\ 54 \end{pmatrix},$$

$$C_5^2 = \begin{pmatrix} 7 & 5 & 9 \\ 1 & 4 & 3 \\ 2 & 3 & 5 \end{pmatrix} \begin{pmatrix} 43 \\ 8 \\ 10 \end{pmatrix} \bmod 61 = \begin{pmatrix} 24 \\ 33 \\ 34 \end{pmatrix}.$$

Diperoleh cipherteks kedua yang berkorespondensi dengan nilai 31, 54, 23, 0, 4, 49, 54, 60, 51, 22, 37, 54, 24, 33, 34. Selanjutnya, cipherteks kedua dienkripsi menggunakan persamaan-persamaan konversi suhu sehingga diperoleh cipherteks-cipherteks terakhir sebagai berikut:

a. Enkripsi menggunakan persamaan konversi suhu dari celcius ke fahrenheit, kelvin, dan reamur

Berdasarkan hasil pada Tabel 3, diperoleh cipherteks terakhir dengan menggunakan konversi suhu dari celcius ke fahrenheit, kelvin, dan reamur, yaitu "87,8F129,2F73,4F32F39,2F120,2F129,2F140F123,8F 71,6F98,6F129,2F75,2F91,4F93,2F", "304K327K296K 273K277K322K327K333K324K295K310K327K297K 306K307K", dan "24,8R43,2R18,4R0R3,2R 39,2R43,2R 48R40,8R17,6R29,6R43,2R19,2R26,4R27,2R".

Tabel 3. Hasil enkripsi menggunakan persamaan konversi suhu dari celcius ke fahrenheit, kelvin, dan reamur

i	C_i^2	C_i^3 (F)	C_i^3 (K)	C_i^3 (R)
1	31	87,8F	304K	24,8R
2	54	129,2F	327K	43,2R
3	23	73,4F	296K	18,4R
4	0	32F	273K	0R
5	4	39,2F	277K	3,2R
6	49	120,2F	322K	39,2R
7	54	129,2F	327K	43,2R
8	60	140F	333K	48R
9	51	123,8F	324K	40,8R
10	22	71,6F	295K	17,6R
11	37	98,6F	310K	29,6R
12	54	129,2F	327K	43,2R
13	24	75,2F	297K	19,2R
14	33	91,4F	306K	26,4R
15	34	93,2F	307K	27,2R

b. Enkripsi menggunakan persamaan konversi suhu dari fahrenheit ke celcius, kelvin, dan reamur

Berdasarkan hasil pada Tabel 4, diperoleh cipherteks terakhir dengan menggunakan konversi suhu dari fahrenheit ke celcius, kelvin, dan reamur, yaitu "-0,56C12,22C-5C-17,78C-15,56C9,44C12,22C15,56C 10,56C-5,56C2,78C12,22C-4,44C0,56C1,11C", "272,44K285,22K268K255,22K257,44K282,44K285,2 2K288,56K283,56K267,44K275,78K285,22K268,56K 273,56K274,11K", dan "-0,44R9,78R-4R-14,22R-12,44R 7,56R9,78R12,44R8,44R-4,44R2,22R9,78R-3,56R0,44R0,89R".

Tabel 4. Hasil enkripsi menggunakan persamaan konversi suhu dari fahrenheit ke celcius, kelvin, dan reamur

i	C_i^2	C_i^3 (C)	C_i^3 (K)	C_i^3 (R)
1	31	-0,56C	272,44K	-0,44R
2	54	12,22C	285,22K	9,78R
3	23	-5C	268K	-4R
4	0	-17,78C	255,22K	-14,22R
5	4	-15,56C	257,44K	-12,44R
6	49	9,44C	282,44K	7,56R
7	54	12,22C	285,22K	9,78R
8	60	15,56C	288,56K	12,44R
9	51	10,56C	283,56K	8,44R
10	22	-5,56C	267,44K	-4,44R
11	37	2,78C	275,78K	2,22R
12	54	12,22C	285,22K	9,78R
13	24	-4,44C	268,56K	-3,56R
14	33	0,56C	273,56K	0,44R
15	34	1,11C	274,11K	0,89R

c. Enkripsi menggunakan persamaan konversi suhu dari kelvin ke celcius, fahrenheit, dan reamur

Berdasarkan hasil pada Tabel 5, diperoleh cipherteks terakhir dengan menggunakan konversi suhu dari kelvin ke celcius, fahrenheit, dan reamur, yaitu "-242C-219C-250C-273C-269C-224C-219C-213C-222C-251C-236C-219C-249C-240C-239C","-403,6F-362,2F-418F-459,4F-452,2F-371,2F-362,2F-351,4F-367,6F-419,8F-392,8F-362,2F-416,2F-400F-398,2F", dan "-193,6R-175,2R-200R-218,4R-215,2R -179,2R-175,2R-170,4R-177,6R-200,8R-188,8R-175,2R-199,2R -192R-191,2R".

d. Enkripsi menggunakan persamaan konversi suhu dari reamur ke celcius, fahrenheit, dan kelvin

Berdasarkan hasil pada Tabel 6, diperoleh cipherteks terakhir dengan menggunakan konversi suhu dari reamur ke celcius, fahrenheit, dan reamur, yaitu "38,75C67,5C28,75C0C5C61,25C67,5C75C63,75C27, 5C46,25C67,5C30C41,25C42,5C", "101,75F153,5F 83,75F32F41F142,25F153,5F167F146,75F81,5F115,2 5F153,5F86F106,25F108,5F", dan "311,75K340,5K 301,75K273K278K334,25K340,5K348K336,75K300,5 K319,25K340,5K303K314,25K315,5K".

Tabel 5. Hasil enkripsi menggunakan persamaan konversi suhu dari kelvin ke celcius, fahrenheit, dan reamur

i	C_i^2	C_i^3 (C)	C_i^3 (F)	C_i^3 (R)
1	31	-242C	-403,6F	-193,6R
2	54	-219C	-362,2F	-175,2R
3	23	-250C	-418F	-200R
4	0	-273C	-459,4F	-218,4R
5	4	-269C	-452,2F	-215,2R
6	49	-224C	-371,2F	-179,2R
7	54	-219C	-362,2F	-175,2R
8	60	-213C	-351,4F	-170,4R
9	51	-222C	-367,6F	-177,6R
10	22	-251C	-419,8F	-200,8R
11	37	-236C	-392,8F	-188,8R
12	54	-219C	-362,2F	-175,2R
13	24	-249C	-416,2F	-199,2R
14	33	-240C	-400F	-192R
15	34	-239C	-398,2F	-191,2R

Tabel 6. Hasil enkripsi menggunakan persamaan konversi suhu dari reamur ke celcius, fahrenheit, dan kelvin

i	C_i^2	C_i^3 (C)	C_i^3 (F)	C_i^3 (K)
1	31	38,75C	101,75F	311,75K
2	54	67,5C	153,5F	340,5K
3	23	28,75C	83,75F	301,75K
4	0	0C	32F	273K
5	4	5C	41F	278K
6	49	61,25C	142,25F	334,25K
7	54	67,5C	153,5F	340,5K
8	60	75C	167F	348K
9	51	63,75C	146,75F	336,75K
10	22	27,5C	81,5F	300,5K
11	37	46,25C	115,25F	319,25K
12	54	67,5C	153,5F	340,5K
13	24	30C	86F	303K
14	33	41,25C	106,25F	314,25K
15	34	42,5C	108,5F	315,5K

3.2. Proses Dekripsi

Cipherteks yang digunakan pada proses dekripsi adalah cipherteks yang telah diperoleh pada proses enkripsi sesuai dengan persamaan konversi suhu yang digunakan. Untuk memperoleh plainteks pertama, digunakan kebalikan dari persamaan konversi suhu pada proses enkripsi.

a. Dekripsi menggunakan persamaan konversi suhu dari fahrenheit, kelvin, dan reamur ke celcius

Cipherteks yang digunakan adalah "87,8F129,2F73,4F32F39,2F120,2F129,2F140F123,8F

71,6F98,6F129,2F75,2F91,4F93,2F", "304K327K296K 273K277K322K327K333K324K295K310K327K297K 306K307K", dan "24,8R43,2R18,4R0R3,2R 39,2R43,2R48R40,8R17,6R29,6R43,2R19,2R26,4R 27,2R". Dengan menggunakan persamaan konversi suhu dari fahrenheit, kelvin, dan reamur ke celcius, diperoleh hasil pada Tabel 7.

Tabel 7. Hasil dekripsi menggunakan persamaan konversi suhu dari fahrenheit, kelvin, dan reamur ke celcius

i	C_i (F)	C_i (K)	C_i (R)	P_i^1
1	87,8	304	24,8	31
2	129,2	327	43,2	54
3	73,4	296	18,4	23
4	32	273	0	0
5	39,2	277	3,2	4
6	120,2	322	39,2	49
7	129,2	327	43,2	54
8	140	333	48	60
9	123,8	324	40,8	51
10	71,6	295	17,6	22
11	98,6	310	29,6	37
12	129,2	327	43,2	54
13	75,2	297	19,2	24
14	91,4	306	26,4	33
15	93,2	307	27,2	34

b. Dekripsi menggunakan persamaan konversi suhu dari celcius, kelvin, dan reamur ke fahrenheit

Cipherteks yang digunakan adalah "272,44K285,22K268K255,22K257,44K282,44K285,2 2K288,56K283,56K267,44K275,78K285,22K268,56K2 73,56K274,11K", dan "-0,44R9,78R-4R-14,22R-12,44R7,56R9,78R12,44R8,44R-4,44R2,22R9,78R-3,56R0,44R0,89R". Dengan menggunakan persamaan konversi suhu dari celcius, kelvin, dan reamur ke fahrenheit, diperoleh hasil pada Tabel 8.

c. Dekripsi menggunakan persamaan konversi suhu dari celcius, fahrenheit, dan reamur ke kelvin

Cipherteks yang digunakan adalah "-242C-219C-250C-273C-269C-224C-219C-213C-222C-251C-236C-219C-249C-240C-239C", "-403,6F-362,2F-418F-459,4F-452,2F-371,2F-362,2F-351,4F-367,6F-419,8F-392,8F-362,2F-416,2F-400F-398,2F", dan "-193,6R-175,2R-200R-218,4R-215,2R-179,2R-175,2R-170,4R-177,6R-200,8R-188,8R-175,2R-199,2R-192R-191,2R". Dengan menggunakan persamaan konversi suhu dari celcius, fahrenheit, dan reamur ke kelvin, diperoleh hasil pada Tabel 9.

Tabel 8. Hasil dekripsi menggunakan persamaan konversi suhu dari celcius, kelvin, dan reamur ke fahrenheit

i	C_i (C)	C_i (K)	C_i (R)	P_i^1
1	-0,56C	272,44	-0,44	31
2	12,22C	285,22	9,78	54
3	-5C	268	-4	23
4	-17,78C	255,22	-14,22	0
5	-15,56C	257,44	-12,44	4
6	9,44C	282,44	7,56	49
7	12,22C	285,22	9,78	54
8	15,56C	288,56	12,44	60
9	10,56C	283,56	8,44	51
10	-5,56C	267,44	-4,44	22
11	2,78C	275,78	2,22	37
12	12,22C	285,22	9,78	54
13	-4,44C	268,56	-3,56	24
14	0,56C	273,56	0,44	33
15	1,11C	274,11	0,89	34

Tabel 9. Hasil dekripsi menggunakan persamaan konversi suhu dari celcius, fahrenheit, dan reamur ke kelvin

i	C_i (C)	C_i (F)	C_i (R)	P_i^1
1	-242	-403,6	-193,6	31
2	-219	-362,2	-175,2	54
3	-250	-418	-200	23
4	-273	-459,4	-218,4	0
5	-269	-452,2	-215,2	4
6	-224	-371,2	-179,2	49
7	-219	-362,2	-175,2	54
8	-213	-351,4	-170,4	60
9	-222	-367,6	-177,6	51
10	-251	-419,8	-200,8	22
11	-236	-392,8	-188,8	37
12	-219	-362,2	-175,2	54
13	-249	-416,2	-199,2	24
14	-240	-400	-192	33
15	-239	-398,2	-191,2	34

d. Dekripsi menggunakan persamaan konversi suhu dari celcius, fahrenheit, dan kelvin ke reamur

Cipherteks yang digunakan adalah "38,75C67,5C28,75C0C5C61,25C67,5C75C63,75C27,5C46,25C67,5C30C41,25C42,5C", "101,75F153,5F83,75F32F41F142,25F153,5F167F146,75F81,5F115,25F153,5F86F106,25F108,5F", dan "311,75K340,5K301,75K273K278K334,25K340,5K348K336,75K300,5K319,25K340,5K303K314,25K315,5K". Dengan menggunakan persamaan konversi suhu dari celcius, fahrenheit, dan kelvin ke reamur, diperoleh hasil pada Tabel 10.

Tabel 10. Hasil dekripsi menggunakan persamaan konversi suhu dari celcius, fahrenheit, dan kelvin ke reamur

i	C_i (C)	C_i (F)	C_i (K)	P_i^1
1	38,75	101,75	311,75	31
2	67,5	153,5	340,5	54
3	28,75	83,75	301,75	23
4	0	32	273	0
5	5	41	278	4
6	61,25	142,25	334,25	49
7	67,5	153,5	340,5	54
8	75	167	348	60
9	63,75	146,75	336,75	51
10	27,5	81,5	300,5	22
11	46,25	115,25	319,25	37
12	67,5	153,5	340,5	54
13	30	86	303	24
14	41,25	106,25	314,25	33
15	42,5	108,5	315,5	34

Oleh karena itu, diperoleh plainteks pertama yang sama, yaitu plainteks yang berkorespondensi dengan nilai 31, 54, 23, 0, 4, 49, 54, 60, 51, 22, 37, 54, 24, 33, 34. Selanjutnya, digunakan modifikasi algoritma Hill *Cipher* dengan menentukan invers dari matriks kunci terlebih dahulu.

$$\det(\boldsymbol{K})^{-1} \bmod 61 = 37^{-1} \bmod 61 = 33,$$

$$\text{adj}(\boldsymbol{K}) = \begin{pmatrix} 11 & 1 & -5 \\ 2 & 17 & -11 \\ -21 & -12 & 23 \end{pmatrix},$$

$$\boldsymbol{K}^{-1} = 33\begin{pmatrix} 11 & 1 & -5 \\ 2 & 17 & -11 \\ -21 & -12 & 23 \end{pmatrix} \bmod 61$$

$$= \begin{pmatrix} 363 & 33 & -165 \\ 66 & 561 & -363 \\ -693 & -396 & 759 \end{pmatrix} \bmod 61$$

$$= \begin{pmatrix} 58 & 33 & 18 \\ 5 & 12 & 3 \\ 39 & 31 & 27 \end{pmatrix}.$$

Diperoleh invers dari matriks kunci adalah

$$\boldsymbol{K}^{-1} = \begin{pmatrix} 58 & 33 & 18 \\ 5 & 12 & 3 \\ 39 & 31 & 27 \end{pmatrix}.$$

Dengan menggunakan modifikasi algoritma Hill *Cipher* diperoleh hasil sebagai berikut:

$$\boldsymbol{P}_1^2 = \begin{pmatrix} 58 & 33 & 18 \\ 5 & 12 & 3 \\ 39 & 31 & 27 \end{pmatrix}\begin{pmatrix} 31 \\ 54 \\ 23 \end{pmatrix} \bmod 61 = \begin{pmatrix} 29 \\ 18 \\ 27 \end{pmatrix},$$

$$\boldsymbol{P}_2^2 = \begin{pmatrix} 58 & 33 & 18 \\ 5 & 12 & 3 \\ 39 & 31 & 27 \end{pmatrix}\begin{pmatrix} 0 \\ 4 \\ 49 \end{pmatrix} \bmod 61 = \begin{pmatrix} 38 \\ 12 \\ 44 \end{pmatrix},$$

$$\boldsymbol{P}_3^2 = \begin{pmatrix} 58 & 33 & 18 \\ 5 & 12 & 3 \\ 39 & 31 & 27 \end{pmatrix}\begin{pmatrix} 54 \\ 60 \\ 51 \end{pmatrix} \bmod 61 = \begin{pmatrix} 52 \\ 45 \\ 36 \end{pmatrix},$$

$$\boldsymbol{P}_4^2 = \begin{pmatrix} 58 & 33 & 18 \\ 5 & 12 & 3 \\ 39 & 31 & 27 \end{pmatrix}\begin{pmatrix} 22 \\ 37 \\ 54 \end{pmatrix} \bmod 61 = \begin{pmatrix} 53 \\ 45 \\ 47 \end{pmatrix},$$

$$\boldsymbol{P}_5^2 = \begin{pmatrix} 58 & 33 & 18 \\ 5 & 12 & 3 \\ 39 & 31 & 27 \end{pmatrix}\begin{pmatrix} 24 \\ 33 \\ 34 \end{pmatrix} \bmod 61 = \begin{pmatrix} 43 \\ 8 \\ 10 \end{pmatrix}.$$

Diperoleh plainteks kedua yang berkorespondensi dengan nilai 29, 18, 27, 38, 12, 44, 52, 45, 36, 53, 45, 47, 43, 8, 10. Selanjutnya, digunakan modifikasi algoritma Vigenere *Cipher* untuk memperoleh plainteks semula. Dengan kata kunci "KONVERSI", diperoleh hasil pada Tabel 11.

Tabel 11. Hasil dekripsi menggunakan modifikasi algoritma Vigenere *Cipher*

i	C_i^1	P_i^3
1	29	19
2	18	4
3	27	14
4	38	17
5	12	8
6	44	27
7	52	34
8	45	37
9	36	26
10	53	39
11	45	32
12	47	26
13	43	39
14	8	52
15	10	53

Berdasarkan hasil pada Tabel 11, diperoleh plainteks semula yang berkorespondensi dengan nilai 19, 4, 14, 17, 8, 27, 34, 37, 26, 39, 32, 26, 39, 52, 53, yaitu "TEORI bilangan 01".

4. Kesimpulan

Kriptografi dengan menggunakan modifikasi algoritma Vigenere *Cipher*, modifikasi algoritma Hill *Cipher*, dan persamaan konversi suhu membuat keamanan suatu pesan lebih terjamin karena dapat menghasilkan 12 cipherteks yang berbeda dari satu plainteks sehingga pesan lebih sulit untuk dipecahkan jika pihak lain tidak

memiliki kunci dan persamaan yang tepat untuk mengenkripsi dan mendekripsi pesan tersebut. Kemudian, kunci dan persamaan konversi suhu yang digunakan pada proses dekripsi haruslah sama dengan kunci yang digunakan pada proses enkripsi agar menghasilkan plainteks semula seperti sebelum dienkripsi. Untuk penelitian selanjutnya, dapat digunakan jumlah karakter yang lebih banyak dan ukuran matriks kunci yang lebih besar.

Daftar Pustaka

1. Rohmanu, A. 2017. Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End of File. *Jurnal Informatika SIMANTIK*, *2*(1), 1–11. Retrieved from https://www.simantik.panca-sakti.ac.id/index.php/simantik/article/view/21
2. Sumandri. 2017. Studi Model Algoritma Kriptografi Klasik dan Modern. In *Seminar Matematika dan Pendidikan Matematika UNY*.
3. Candra C. 2016. Keamanan Data dengan Metode Kriptografi Kunci Publik. *Jurnal TIMES*, *5*(2), 11–15. Retrieved from https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/548
4. Munir, R. 2019. *Kriptografi* (2nd ed.). Bandung: Penerbit Informatika Bandung.
5. Irawan, M. D. 2017. Implementasi Kriptografi Vigenere Cipher dengan PHP. *Jurnal Teknologi Informasi*, *1*(1), 11. https://doi.org/10.36294/jurti.v1i1.21.
6. Harahap, M. K. 2016. Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher dan One Time Pad. *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*. https://doi.org/doi:10.30743/infotekjar.v1i1.43.
7. Nepla Bima Putra, Cirya Andika, B., Daniata Purba, A., & Ridwan, M. 2023. Implementasi Sandi Vigenere Cipher dalam Mengenkripsikan Pesan. *JOCITIS-Journal Science Infomatica and Robotics*, *1*(1), 42–50. Retrieved from https://jurnal.ittc.web.id/index.php/jct/article/view/25
8. Nahar, K., & Chakraborty, P. 2020. A Modified Version of Vigenere Cipher using 95x95 Table. *International Journal of Engineering and Advanced Technology*, *9*(5), 1144–1148. https://doi.org/10.35940/ijeat.E9941.069520.
9. Pardede, A. M. H. 2017. Algoritma Vigenere Cipher dan Hill Cipher dalam Aplikasi Keamanan Data pada File Dokumen. *Jurnal Teknik Informatika Kaputama (JTIK)*. Retrieved from https://doi.org/10.31227/osf.io/7h36y
10. Wowor, A. D. 2013. Modifikasi Kriptografi Hill Cipher Menggunakan Convert Between Base. In *Seminar Nasional Sistem Informasi Indonesia (SESINDO)*. Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember.
11. Sharma, S. K. 2020. An Application of Hill Cipher by Using Modular Matrices. *Engineering and Technology Journal for Research and Innovation (ETJRI)*, *II*(II), 32–34.
12. Amijaya, F. D. T., Syaripuddin, S., A'yun, Q. Q., Nasution, Y. N., Wasono, W., & Huda, Moh. N. 2022. Hill Cipher algorithm using two keywords and 94 ASCII characters. In *AIP Conf. Proc* (p. 050006). https://doi.org/10.1063/5.0111696.
13. Nugraha, Y. W., Thresye, T., & Soesanto, O. 2023. Modifikasi Hill Cipher dengan Menggunakan Matriks Kunci Orthogonal dan Transposition Substitution Left Right Shift (TSLRS). *Epsilon: Jurnal Matematika Murni Dan Terapan*, *17*(1).
14. Ginting, V. S. 2020. Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa. *Jurnal Teknologi Informasi*, *4*(2), 241–246. https://doi.org/10.36294/jurti.v4i2.1365.
15. Handoko, L. B., & Abdussalam, A. 2022. Text Security Using Vigenere Cipher and Hill Cipher. *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, *19*(1), 37. https://doi.org/10.36080/bit.v19i1.1790.
16. Haris, C. A., & Ariyus, D. 2020. Kombinasi dan Modifikasi Vigenere Cipher dan Hill Cipher Menggunakan Metode Hybrid Kode Pos, Trigonometri, dan Konversi Suhu Sebagai Pengamanan Pesan. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, *15*(2), 90. https://doi.org/10.30872/jim.v15i2.3746.