PRISMA 4 (2021): 548-552
PRISMA, Prosiding Seminar Nasional Matematika
https://journal.unnes.ac.id/sju/index.php/prisma/
ISSN 2613-9189

Pengkodean Teks Menggunakan Kombinasi *Hill Cipher* dan Operasi *XOR*

Rif'atul Makhomah[a,*], Kiswara Agung Santoso [a], Ahmad Kamsyakawuni[a]

[a] *Universitas Jember, Jl. Kalimantan 37 Jember 68121, Indonesia*

* *Alamat Surel: kiswaras@gmail.com*

Abstrak

Perkembangan zaman membuat teknologi infomasi dan komunikasi semakin maju. Penting untuk menjaga keamanan pesan agar tidak diketahui oleh pihak lain salah satunya dengan menggunakan ilmu kriptografi. Salah satu teknik kriptografi klasik yang memanfaatkan aritmetika modulo dan operasi matriks yaitu algoritma *hill cipher*, dimana untuk proses enkripsi dan dekripsi menggunakan kunci matriks. Disini penulis tertarik mengkombinasikan *hill cipher* dengan operasi *XOR*. *Plaintext* awal di-*XOR*-kan dengan jumlah setiap kolom kunci matriks yang nantinya akan menjadi *plaintext* baru dilanjutkan dengan enkripsi dan dekripsi *hill cipher*.

Kata kunci:

Kriptografi, *Hill Cipher, XOR.*

1. Pendahuluan

Perkembangan zaman membuat teknologi informasi dan komunikasi semakin maju. Proses bertukar pesan atau informasi menjadi semakin mudah dilakukan. Dalam proses bertukar pesan sangat penting menjaga keamanan pesan atau informasi agar pesan tersebut tidak dapat dimengerti oleh pihak lain maupun pihak yang tidak berwenang. Kriptografi merupakan salah satu metode yang banyak digunakan saat ini. Kriptografi Didefisikan sebagai ilmu sekaligus seni untuk menjaga keamanan pesan agar tidak diketahui oleh pihak yang tidak berwenang.

Kriptografi memiliki dua jenis, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik umumnya beroperasi dalam mode karakter. Salah satu algoritma kriptografi klasik yaitu *hill chiper*. *Hill cipher* memanfaatkan aritmetika modulo dan operasi matriks, dimana pada algoritma *hill cipher* kunci yang digunakan untuk proses enkripsi dan dekripsi adalah matriks. Berikut merupakan rumus yang digunakan dalam proses enkripsi dan dekripsi *hill cipher* dapat dilihat pada persamaan (1) dan persamaan (2).

$$C_i = (K.P_i)\ mod\ 26 \quad (1)$$

$$P_i = (K^{-1}.C_i) mod\ 26 \quad (2)$$

Kriptografi modern beroperasi dalam bentuk mode bit yang artinya semua data dan informasi baik *plaintext*, kunci, dan *chipertext* dinyatakan dalam rangkaian bit biner 0 dan 1. Hasil enkripsi dan dekripsi algoritma kriptografi modern dinyatakan dalam rangakaian bit. Salah satu algoritma modern yang sering digunakan yaitu operasi *XOR* yang mana setiap bit *plaintext* di-*XOR*-kan dengan setiap bit kunci.

Beberapa penelitian yang dilakukan terkait modifikasi *hill cipher* maupun penggabungan *Hill cipher* dengan algoritma lain. Rahmawati (2017) melakukan penelitian dengan judul "Penggabungan *Vigenere Cipher* dengan *Hill Cipher* pada Pengkodean *Plaintext* dengan Kunci Bertahap". Penelitian ini membahas tentang penggabungan *vigenere cipher* dan *hill cipher* menggunakan kunci bertahap untuk proses pengkodean pesan teks. Mujaddid dan Sumarsono (2017) melakukan penelitian dengan judul "*A Modifying of Hill Cipher Algorithm with 3 Substitution Caesar Cipher*" penelitian membahas tentang modifikasi *hill cipher* dengan substitusi *caesar cipher*. Berdasarkan beberapa penelitian

To cite this article:
Makhomah, R., Santoso, K. A., & Kamsyakawuni, A. (2021). Pengkodean Teks Menggunakan Kombinasi *Hill Cipher* dan Operasi *XOR*. *PRISMA, Prosiding Seminar Nasional Matematika 4*, 548-552

diatas, penulis akan mengkombinasikan algoritma *hill cipher* dengan operasi *XOR*. Pada proses pengkodean teks dengan menggunakan *hill cipher*, *plaintext* akan di-*XOR*-kan terlebih dahulu dengan penjumlahan tiap kolom kunci matriks yang hasilnya akan dilakukan operasi *hill cipher*.

2. Metode

Data yang digunakan pada penelitian ini merupakan data pada tabel ASCII *printable characters* baik karakter maupun binernya. Terdapat dua *plaintext* yang digunakan dalam penelitian ini yaitu *plaintext* asli dan *plaintext* hasil operasi *XOR* antara *plaintext* asli dan jumlah tiap kolom kunci matriks.

2.1 Pembentukan kunci hill cipher

Kunci matriks yang digunakan merupakan matriks 3 x 3. Matriks kunci harus *invertible* yaitu memiliki *invers* $K.K^{-1}$. Jika kunci tidak memiliki *invers* maka membentuk kunci matriks lain, hal ini dilakukan agar *ciphertext* dapat didekripsi.

2.2 Operasi Enkripsi XOR

Dalam tahap ini *plaintext* akan di-*XOR*-kan dengan jumlah tiap kolom kunci matriks. Hasil penjumlahan kolom di-*XOR*-kan dengan tiap 3 karakter *plaintext*.. Kemudian *plaintext* dan kunci dikonversi ke dalam bentuk biner. Hasil dari operasi *XOR* akan menjadi *plaintext* baru (*P*`) yang digunakan dalam proses enkripsi. Rumus operasi *XOR* dapat dilihat pada persamaan (3):

$$P_i` = P_i \oplus K \quad (3)$$

2.3 Proses enkripsi

Plaintext yang digunakan merupakn *plaintext* hasil operasi *XOR*. Rumus yang digunakan mengalami perubahan yaitu modulo 95 sesuai dengan jumlah karakter dalam tabel ASCII *printable characters* dari 32-126. Dilakukan penambahan dan pengurangan 32 agar hasil selalu dalam rentang 32-126. Rumus proses enkripsi dapat dilihat pada persamaan (4):

$$C_i = \big(K.(P`_i - 32)\big) mod\ 95 + 32 \quad (4)$$

2.4 Proses dekripsi

Proses dekripsi sama dengan proses enkripsi. Kunci yang digunakan dalam proses dekripsi merupakan *invers* dari matriks kunci. Berikut rumus dekripsi dapat dilihat pada persamaan (5):

$$P`_i = (K^{-1}.(C_i - 32)) mod\ 95 + 32 \quad (5)$$

2.5 Operasi Dekripsi XOR

Dalam tahap ini hasil dari proses dekripsi dilakukan operasi *XOR*. Hasil dari operasi *XOR* menjadi *plaintext* awal. Operasi ini dilakukan berdasarkan persamaan (6):

$$P_i = P`_i \oplus K \quad (6)$$

3. Hasil dan Pembahasan

Pada penelitian ini data yang digunakan dapat dilihat pada tabel (1).

Tabel 1. Data penelitian

***Plaintext* Awal**	:inya(sp)RIFA#1630
***Plaintext* Hasil XOR**	jzb$QJBB(sp)5504
Kunci Matriks	$\begin{bmatrix}2 & 1 & 3\\1 & 1 & 1\\0 & 1 & 0\end{bmatrix}$
Ciphertext	w+HC#8(sp)j(9@z;P

3.1 Pembentukan Kunci

Kunci yang digunakan merupakan matriks *invertible* yaitu memiliki *invers* $K.K^{-1} = 1$. Misal kunci matriks yang digunakan, yaitu $K = \begin{bmatrix}2 & 1 & 3\\1 & 1 & 1\\0 & 1 & 0\end{bmatrix}$ invers dari kunci matriks yaitu $K^{-1} = \begin{bmatrix}-1 & 3 & -2\\0 & 0 & 1\\1 & -2 & 1\end{bmatrix}$.

3.2 Operasi Enkripsi XOR

Plaintext awal " **kuncinya(sp)RIFA#1630** " di-*XOR*-kan dengan jumlah setiap kolom kunci matriks yaitu 3, 3, 4. *Plaintext* dan jumlah setiap kolom kunci matriks dikonversikan kedalam bentuk biner, karena operasi *XOR* hanya beroperasi pada biner. Berikut proses operasi *XOR* antara *plaintext* awal dan kunci (3, 3, 4) dapat dilihat pada tabel (2).

Tabel 2. Proses enkripsi *XOR*

Plaintext	**Biner P_i**	**K**	**Biner $P`_i$**	**$P`_i$**
k	01101011	00000011	01101000	h
u	01110101	00000011	01110110	v
n	01101110	00000100	01101010	j
c	01100011	00000011	01100000	`
i	01101001	00000011	01101010	j
n	01101110	00000100	01101010	j
y	01111001	00000011	01111010	z
a	01100001	00000011	01100010	b
(sp)	00100000	00000100	00100100	$
R	01010010	00000011	01010001	Q
I	01001001	00000011	01001010	J
F	01000110	00000100	01000010	B
A	01000001	00000011	01000010	B
#	00100011	00000011	00100000	(sp)
1	00110001	00000100	00110101	5
6	00110110	00000011	00110101	5
3	00110011	00000011	00110000	0
0	00110000	00000100	00110100	4

$P`$ dari hasil operasi *XOR* ini akan menjadi *plaintext* baru, yaitu " hvj`jjzb$QJBB(sp)5504" yang akan digunakan dalam proses enkripsi.

3.3 Proses Enkripsi

Pada tahap ini *plaintext* baru yaitu " hvj`jjzb$QJBB(sp)5504" dilakukan proses enkripsi menggunakan algoritma *hill cipher*. *Plaintext* dikonversi ke dalam bentuk desimal karena *hill cipher* hanya beroperasi dalam bentuk desimal. Konversi desimal dapat dilihat pada tabel (3).

Tabel 3. Konversi *plaintext* ke desimal

Karakter	**Desimal**
h	104
v	118
j	106
`	96
.	.
4	52

Plaintext dibagi menjadi 3 karakter per blok sesuai dengan kunci matriks 3 x 3 Berikut proses enkripsi:

$$C_1 = \left(\begin{bmatrix}2 & 1 & 3\\ 1 & 1 & 1\\ 0 & 1 & 0\end{bmatrix} \times \left(\begin{bmatrix}104\\ 118\\ 106\end{bmatrix} - 32\right)\right) \bmod 95 + 32 = \begin{bmatrix}74\\ 43\\ 118\end{bmatrix} = \text{J+v}$$

$$C_2 = \left(\begin{bmatrix}2 & 1 & 3\\ 1 & 1 & 1\\ 0 & 1 & 0\end{bmatrix} \times \left(\begin{bmatrix}96\\ 106\\ 106\end{bmatrix} - 32\right)\right) \bmod 95 + 32 = \begin{bmatrix}46\\ 118\\ 106\end{bmatrix} = \text{vj}$$

$$C_3 = \left(\begin{bmatrix}2 & 1 & 3\\ 1 & 1 & 1\\ 0 & 1 & 0\end{bmatrix} \times \left(\begin{bmatrix}122\\ 98\\ 36\end{bmatrix} - 32\right)\right) \bmod 95 + 32 = \begin{bmatrix}70\\ 66\\ 98\end{bmatrix} = \text{FBb}$$

.
.
.

$$C_6 = \left(\begin{bmatrix}2 & 1 & 3\\ 1 & 1 & 1\\ 0 & 1 & 0\end{bmatrix} \times \left(\begin{bmatrix}53\\ 48\\ 52\end{bmatrix} - 32\right)\right) \bmod 95 + 32 = \begin{bmatrix}120\\ 58\\ 48\end{bmatrix} = \text{x:0}$$

Setelah proses enkripsi didapatkan *ciphertext* " J+v,vjFBb6~J&8(sp)x:0" yang akan digunakan dalam proses dekripsi.

3.4 Proses Dekripsi

Proses dekripsi *hill cipher* dilakukan dengan *ciphertext* " J+v,vjFBb6~J&8(sp)x:0" dan kunci matriks *invers*. *Ciphertext* di konversikan kedalam bentuk desimal, dapat dilihat pada tabel (4).

Tabel 4. Konversi *ciphertext* ke desimal

Karakter	Desimal
J	74
+	43
v	118
,	46
.	.
0	48

Berikut proses dekripsinya:

$$P_1 = \left(\begin{bmatrix}-1 & 3 & -2\\ 0 & 0 & 1\\ 1 & -2 & 1\end{bmatrix} \times \left(\begin{bmatrix}74\\ 43\\ 118\end{bmatrix} - 32\right)\right) \bmod 95 + 32 = \begin{bmatrix}104\\ 118\\ 106\end{bmatrix} = \text{hvj}$$

$$P_2 = \left(\begin{bmatrix}-1 & 3 & -2\\ 0 & 0 & 1\\ 1 & -2 & 1\end{bmatrix} \times \left(\begin{bmatrix}46\\ 118\\ 106\end{bmatrix} - 32\right)\right) \bmod 95 + 32 = \begin{bmatrix}96\\ 106\\ 106\end{bmatrix} = \text{`jj}$$

$$P_3 = \left(\begin{bmatrix}-1 & 3 & -2\\ 0 & 0 & 1\\ 1 & -2 & 1\end{bmatrix} \times \left(\begin{bmatrix}70\\ 66\\ 98\end{bmatrix} - 32\right)\right) \bmod 95 + 32 = \begin{bmatrix}122\\ 98\\ 36\end{bmatrix} = \text{zb\$}$$

.
.
.

$$P_6 = \left(\begin{bmatrix}-1 & 3 & -2\\ 0 & 0 & 1\\ 1 & -2 & 1\end{bmatrix} \times \left(\begin{bmatrix}120\\ 58\\ 48\end{bmatrix} - 32\right)\right) \bmod 95 + 32 = \begin{bmatrix}53\\ 48\\ 52\end{bmatrix} = 504$$

Setelah proses dekripsi didapatkan *plaintext* "hvj`jjzb$QJBB(sp)5504" *Plaintext* tersebut digunakan untuk mendapatkan *plaintext* awal.

3.5 Operasi Dekripsi XOR

Plaintext " hvj`jjzb$QJBB(sp)5504" akan di-*XOR*-kan dengan 3, 3, 4 untuk mendapatkan *plaintext* awal. Proses *XOR* dapat dilihat pada tabel (5).

Tabel 5. Proses dekripsi *XOR*

$P_i^{`}$	Biner $P_i^{`}$	K	Biner P_i	Plaintext

h	01101000	00000011	01101011	k
v	01110110	00000011	01110101	u
j	01101010	00000100	01101110	n
`	01100000	00000011	01100011	c
j	01101010	00000011	01101001	i
j	01101010	00000100	01101110	n
z	01111010	00000011	01111001	y
b	01100010	00000011	01100001	a
$	00100100	00000100	00100000	(sp)
Q	01010001	00000011	01010010	R
J	01001010	00000011	01001001	I
B	01000010	00000100	01000110	F
B	01000010	00000011	01000001	A
(sp)	00100000	00000011	00100011	#
5	00110101	00000100	00110001	1
5	00110101	00000011	00110110	6
0	00110000	00000011	00110011	3
4	00110100	00000100	00110000	0

Hasil operasi *XOR* ini kembali menjadi *plaintext* baru yaitu " kuncinya(sp)RIFA#1630 ".

3.7 Pembahasan

Proses kombinasi algoritma *hill cipher* dan operasi *XOR* dilakukan dengan *plaintext* awal di-*XOR*-kan dengan jumlah tiap kolom kunci matriks. Hasil dari operasi *XOR* menjadi *plaintext* baru yang digunakan dalam proses enkripsi *hill cipher*. Terdapat penjumlahan dan pengurangan pada *plaintext* sebanyak 32, hal ini dilakukan agar hasil enkripsi berada pada rentang 32 sampai 126 sesuai dengan tabel ASCII *printable characters* karena data yang digunakan merupakan data pada tabel ASCII pintable character. Terdapat perubahan modulo menjadi modulo 95 karena jumlah karakter pada tabel ASCII *printable characters* sebanyak 95.

4. Simpulan

Proses kombinasi algoritma *hill cipher* dan operasi *XOR* dilakukan dengan *plaintext* awal di-*XOR*-kan dengan jumlah tiap kolom kunci matriks yaitu 3, 3, 4. Hasil dari operasi *XOR* menjadi *plaintext* baru yang digunakan dalam proses enkripsi *hill cipher*. Terdapat penjumlahan dan pengurangan pada *plaintext* sebanyak 32 dan perubahan modulo menjadi modulo 95. Hal ini dilakukan agar sesuai dengan jumlah karakter pada tabel ASCII *printable characters*.

Daftar Pustaka

Mujaddid, A., & Sumarsono, S. (2017, October). A Modifying of Hill Cipher Algorithm with 3 Substitution Caesar Cipher. In *Proceeding International Conference on Science and Engineering* (Vol. 1, pp. 157-163).

Rahmawati, R. (2017). Penggabungan Vigenere Cipher dengan Hill Cipher pada Pengkodean Plaintext dengan Kunci Bertahap. Jember: Universitas Jember.

Setyaningsih, E. (2015). Kriptografi dan Implementasinya Menggunakan MATLAB. Yogyakarta: Andi Offset.

Suhardi, S. (2018). Aplikasi Kriptografi Data Sederhana dengan Metode Exlusive-or (Xor). *Jurnal Teknovasi: Jurnal Teknik dan Inovasi*, *3*(2), 23-31.