JKMA
Jurnal Kajian Matematika dan Aplikasinya
VOLUME 4 NOMOR 1, January 2023
e-ISSN: 2722-7650. http://journal2.um.ac.id/index.php/jkma

IMPLEMENTASI MATRIKS ATAS GELANGGANG $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$ PADA KRIPTOGRAFI CIPHER HILL

Ikhsan Abdul Ro'uf[1,*], Mukhammad Solikhin[1], Lita Wulandari Aeli[1], Andi Daniah Pahrany[1], Irmatul Hasanah[2]
[1]Universitas Negeri Malang
[2]Universitas Islam Negeri Sultan Maulana Hasanuddin Banten

Email : ikhsan.abdul.2003126@students.um.ac.id (*I. A. Ro'uf*), mukhammad.solikhin.fmipa@um.ac.id (*M. Solikhin*), lita.wulandariaeli.fmipa@um.ac.id (*L. W. Aeli*), andi.daniah.fmipa@um.ac.id (*A. D. Pahrany*), irmatul.hasanah@uinbanten.ac.id (*I. Hasanah*)
*****Corresponding Author

Abstract
Cryptography is a method for securing data or information from data leaks. In cryptography, there are two important processes, namely, the encryption and decryption processes. Encryption is the process of changing plaintext into ciphertext using certain keys and algorithms, while decryption is the process of changing ciphertext into plaintext using keys and algorithms that match the encryption. There is a cryptosystem that is well known, namely Cipher Hill. Cipher Hill uses a square matrix for the encryption and decryption process. In this research, an $m \times n$ −sized matrix will be used over the Direct Sum ring $Z_p \oplus Z_q \oplus Z_r$ to expand the Cipher Hill algorithm. The author also uses the pseudoinverse concept to find the inverse of an $m \times n$ matrix. By using an $m \times n$ matrix, the encryption results allow the length of the plaintext to be different from the length of the ciphertext.

Keywords: *Cipher Hill, Cryptography, Decryption, Encryption, Direct Sum, Pseudoinvers*

Submitted:15 March 2023; Revised:15 July 2023; Accepted Publication: 6 September 2023;
Published Online: October 2023
DOI: 10.17977/um055v4i1p15-23

PENDAHULUAN

Kriptografi adalah suatu metode untuk mengamankan data atau informasi dari kebocoran data. Kriptografi mengubah suatu data menjadi suatu bentuk yang mungkin tidak memiliki makna tertentu, sehingga menyulitkan seseorang untuk megetahui isi data tersebut. Untuk menjalankan suatu metode Kriptografi diperlukan adanya sistem kripto yang terdiri dari *plaintext* (teks yang akan dienkripsi), *ciphertext* (teks hasil enkripsi), kunci, algoritma enkripsi, dan algoritma dekripsi (Buchmann, 2001). Proses enkripsi adalah proses mengubah *plaintext* menjadi *ciphertext* dengan menggunakan kunci dan algoritma tertentu, sedangkan proses dekripsi adalah proses mengubah *ciphertext* menjadi *plaintext* dengan menggunakan kunci dan algoritma yang sesuai dengan ekripsi.

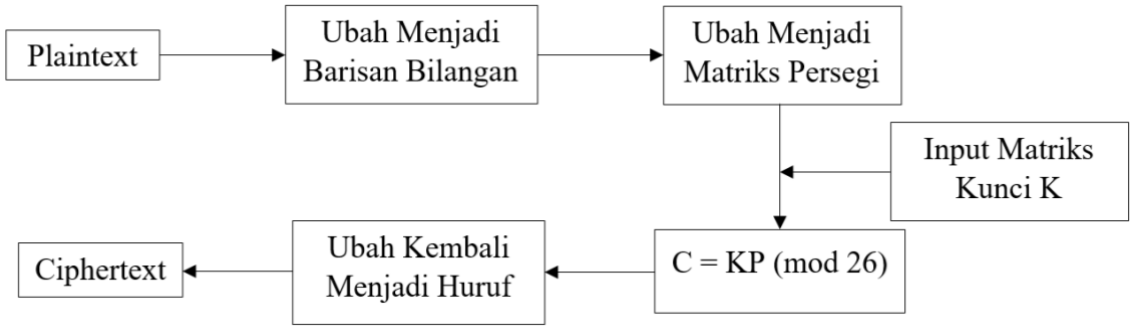
Salah satu sistem kripto yang sudah lama dikenal yaitu Cipher Hill. Cipher Hill pertama kali dikenalkan oleh Lester S. Hill pada tahun 1929 (Hill, 1929). Algoritma Cipher Hill memerlukan sebuah tabel korespondensi $1-1$ antara alfabet dengan suatu gelanggang $\mathbb{Z}_{26}$ yang digunakan untuk mengubah *plaintext* menjadi barisan angka. Tabel 1 merupakan contoh tabel korespondesi $1-1$ antara alfabet dan gelanggang $\mathbb{Z}_{26}$.

Tabel 1. Contoh tabel pemetaan $1-1$ dari alfabet ke gelanggang $\mathbb{Z}_{26}$

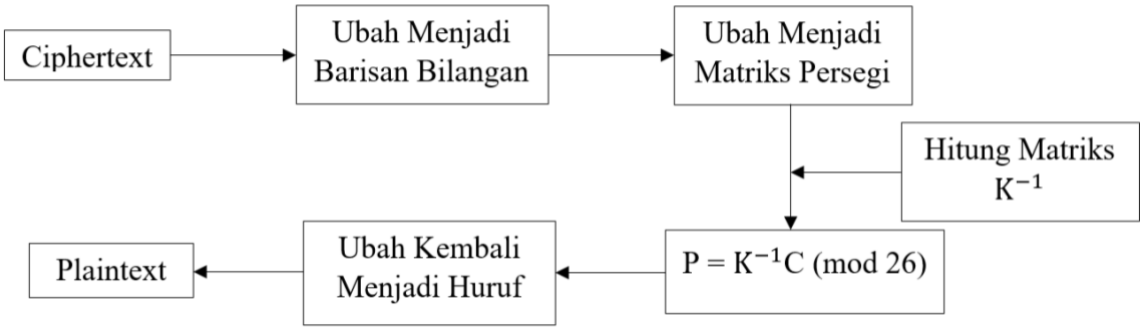
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Dengan menggunakan tabel tersebut proses enkripsi Cipher Hill dilakukan dengan cara mengubah *plaintext* p dengan panjang n menjadi barisan bilangan yang bersesuaian dengan Tabel 1. Selanjutnya, barisan angka tersebut diubah menjadi matriks berukuran $n \times n$. Langkah selanjutnya adalah mengalikan matriks yang diperoleh dengan matriks invertibel K berukuran $n \times n$ atas $\mathbb{Z}_{26}$ yang menghasilkan matriks *ciphertext*. Matriks *ciphertext* yang diperoleh selanjutnya diubah mejadi barisan bilangan dan diubah kembali menjadi teks menggunakan Tabel 1 sehingga dihasilkan *ciphertext* c.

Sedangkan untuk proses dekripsi dilakukan dengan cara serupa yaitu mengubah *ciphertext* c menjadi barisan bilangan kemudian diubah menjadi matriks persegi. Selanjutnya, matriks tersebut dikalikan dengan invers dari matriks kunci K sehingga diperoleh matriks yang sama dengan matriks *plaintext* P. Langkah terakhir yaitu mengubah matriks *plaintext* menjadi kata yang sesuai Tabel 1 sehingga diperoleh *plaintext* p. Secara matematis, algoritma Cipher Hill dituliskan seperti pada Gambar 1 dan Gambar 2.



Gambar 1. Skema proses enkripsi algoritma Cipher Hill



Gambar 2. Skema proses dekripsi algoritma Cipher Hill

Algoritma Cipher Hill pada Gambar 1 dan Gambar 2 memiliki beberapa kelemahan yaitu matriks kunci haruslah matriks invertibel dan persegi sehingga matriks kunci yang dapat digunakan terbatas. Selain itu, matriks kunci adalah matriks atas gelanggang $\mathbb{Z}_{26}$ sehingga banyaknya matriks invertibel juga semakin sedikit. Kelemahan yang lain adalah terdapat beberapa kata yang tidak dapat diubah langsung menjadi matriks persegi, sebagai contoh kata "HAI" tidak dapat diubah secara langsung menjadi matriks persegi sehingga perlu menambah satu huruf agar kata "HAI" dapat diubah menjadi matriks persegi.

Pada penelitian kali ini akan dibahas mengenai implementasi matriks atas gelanggang $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$ untuk memberikan solusi dari permasalahan di atas. Penelitian ini disusun sebagai berikut. Pada bagian 2 akan dijelaskan mengenai gelanggang $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$, pada bagian 3 akan dijelaskan mengenai algoritma Cipher Hill, pada bagian 4 akan dijelaskan mengenai pseudoinvers. Pada bagian terakhir akan dijelaskan mengenai hasil dan pembahasan serta kesimpulan dari penelitian ini.

MATRIKS ATAS GELANGGANG $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$

Misalkan $R_1, R_2, \dots, R_n$ merupakan suatu gelanggang, didefisikan

$$R_1 \oplus R_2 \oplus \dots \oplus R_n = \{(a_1, a_2, \dots, a_n) | a_i \in R_i\}$$

dengan operasi penjumlahan dan perkalian didefinisikan pointwise yaitu

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

dan

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$$

$R_1 \oplus R_2 \oplus \dots \oplus R_n$ disebut dengan *Direct Sum* dari gelanggang $R_1, R_2, \dots, R_n$. (Gallian, 2021)

Dari definisi diatas dapat dibuat matriks atas $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$ yaitu matriks berukuran $m \times n$ dengan entri-entri dari $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$ sebagai contoh adalah $A = \begin{bmatrix} (a_1, b_1, c_1) & (a_2, b_2, c_2) \\ (a_3, b_3, c_3) & (a_4, b_4, c_4) \end{bmatrix}$ adalah matriks 2×2 dengan $a_i \in \mathbb{Z}_p, b_i \in \mathbb{Z}_q$, dan $c_i \in \mathbb{Z}_r$ untuk $i = 1,2,3,4$. Pada teorema berikut akan ditujukkan bahwa matriks atas gelanggang $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$ akan isomorfis dengan *Direct Sum* atas matriks.

Teorema Matriks Atas Direct Sum

Jika $R_1 \oplus R_2 \oplus \dots \oplus R_n$ merupakan direct sum dari gelanggang-gelanggang $R_1, R_2, \dots, R_n$. Maka

$$M_{n \times n}(R_1 \oplus R_2 \oplus \dots \oplus R_s) \cong M_{n \times n}(R_1) \oplus M_{n \times n}(R_2) \oplus \dots \oplus M_{n \times n}(R_s)$$

dengan $M_{n \times n}$ menyatakan matriks berukuran $n \times n$. (Brown, 1993)

Akibat dari teorema tersebut kita dapat memandang matriks atas gelanggang $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$ sebagai tiga matriks yaitu matriks atas gelanggang $\mathbb{Z}_p$, matriks atas gelanggang $\mathbb{Z}_q$, dan matriks atas gelanggang $\mathbb{Z}_r$. Sehingga untuk mencari invers dari matriks atas gelanggang $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$ sama dengan mencari invers untuk ketiga matriks tersebut.

KRIPTOGRAFI CIPHER HILL

Proses enkripsi dan dekripsi dari kriptografi Cipher Hill akan dijelaskan sebagai berikut. Diberikan sebuah *plaintext* p dengan panjang n diubah menjadi barisan angka menggunakan tabel 2 berikut ini. Selanjutnya, barisan angka tersebut diubah menjadi matriks persegi P. Proses enkripsi dilanjutkan dengan mengalikan matriks P dengan matriks kunci K sehingga diperoleh matriks C. Selanjutnya matriks C diubah kembali menjadi barisan angka dan diubah menjadi huruf menggunakan tabel 2. Untuk proses dekripsi, diberikan *ciphertext* c dengan panjang n diubah menjadi barisan angka menggunakan tabel 2 yang selanjutnya diubah menjadi matriks C. Kemudian matriks C yang diperoleh dikalikan dengan matriks K^{-1} sehingga diperoleh matriks P yang selanjutnya akan diubah menjadi barisan angka dan dikembalikan menjadi huruf.

Tabel 2. Contoh tabel pemetaan $1-1$ dari alfabet ke gelanggang $\mathbb{Z}_{26}$

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Sebagai contoh, dengan menggunakan tabel 2 plaintext "SAYA" berkorespondensi dengan barisan bilangan "18,0,24,0" akan dienkripsi dengan menggunakan matriks kunci

$$K = \begin{bmatrix} 3 & 4 \\ 6 & 7 \end{bmatrix}$$

sehingga diperoleh matriks *ciphertext* hasil enkripsi

$$\begin{aligned} C &= KP \ (mod\ 26) \\ &= \begin{bmatrix} 3 & 4 \\ 6 & 7 \end{bmatrix}\begin{bmatrix} 18 & 0 \\ 0 & 24 \end{bmatrix} \ (mod\ 26) \\ &= \begin{bmatrix} 54 & 96 \\ 108 & 168 \end{bmatrix} \ (mod\ 26) \\ &= \begin{bmatrix} 2 & 18 \\ 4 & 12 \end{bmatrix} \end{aligned}$$

dari matriks tersebut diperoleh *ciphertext* "CSEM". Untuk mendekripsi *ciphertext* tersebut digunakan invers dari matriks kunci yaitu

$$K^{-1} = \begin{bmatrix} 15 & 10 \\ 2 & 25 \end{bmatrix}$$

sehingga diperoleh matriks *plaintext* hasil dekripsi

$$\begin{aligned} P &= K^{-1}C \ (mod\ 26) \\ &= \begin{bmatrix} 15 & 10 \\ 2 & 25 \end{bmatrix}\begin{bmatrix} 2 & 18 \\ 4 & 12 \end{bmatrix} \ (mod\ 26) \\ &= \begin{bmatrix} 70 & 390 \\ 104 & 336 \end{bmatrix} \ (mod\ 26) \\ &= \begin{bmatrix} 18 & 0 \\ 0 & 24 \end{bmatrix} \end{aligned}$$

diperoleh *plaintext* yang sama yaitu "SAYA".

Proses enkripsi dan dekripsi dari algoritma Cipher Hill ini dapat dijelaskan secara matematis sebagai berikut, misalkan $\mathcal{P}$ dan $\mathcal{C}$ adalah ruang *plaintext* atas $\mathbb{Z}_{26}$ dan ruang *ciphertext* atas $\mathbb{Z}_{26}$ secara berturut-turut serta $\mathcal{K}$ adalah ruang kunci yang berisi matriks-matriks invertibel atas gelanggang $\mathbb{Z}_{26}$. Diberikan *plaintext* P dengan panjang n serta memilih $K \in \mathcal{K}$ berukuran $n \times n$ sebagai matriks kunci. Proses enkripsi berjalan sebagai berikut, mengubah *plaintext* P menjadi

$$P = [p_1 \ \ p_2 \ \ p_3 \ \ \dots \ \ p_n] \in \mathcal{P}$$

Yang akan diubah menjadi matriks *ciphertext* $C = [c_1 \ \ c_2 \ \ c_3 \ \ \dots \ \ c_n] \in \mathcal{C}$ dengan menggunakan matriks kunci $K = \begin{bmatrix} k_{11} & k_{12} & k_{13} & & k_{1n} \\ k_{21} & k_{22} & k_{23} & \cdots & k_{2n} \\ k_{31} & k_{32} & k_{33} & & k_{3n} \\ & \vdots & & \ddots & \vdots \\ k_{n1} & k_{n2} & k_{n3} & \cdots & k_{nn} \end{bmatrix}$ melalui persamaan

$$C = KP \ (mod\ 26)$$

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} & & k_{1n} \\ k_{21} & k_{22} & k_{23} & \cdots & k_{2n} \\ k_{31} & k_{32} & k_{33} & & k_{3n} \\ & \vdots & & \ddots & \vdots \\ k_{n1} & k_{n2} & k_{n3} & \cdots & k_{nn} \end{bmatrix}\begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_n \end{bmatrix} \ (mod\ 26)$$

Sedangkan proses dekripsi dapat dituliskan melalui persamaan

$$C = KP \ (mod\ 26)$$

$$K^{-1}C\ (mod\ 26) = K^{-1}(KP)\ (mod\ 26)$$
$$K^{-1}C\ (mod\ 26) = P\ (mod\ 26)$$
$$K^{-1}C\ (mod\ 26) = P$$

HASIL DAN PEMBAHASAN

Pada bagian ini akan dibahas mengenai matriks invers diperluas (pseudoinvers) menggunakan teorema Singular Value Decomposition (SVD).

Singular Value Decomposition (SVD)

Misalkan A matriks berukuran $m \times n$ dengan rank k, maka A dapat dituliskandalam bentuk $A = U\Sigma V^T$, dengan Σ merupakan matriks berukuran $m \times n$ yang berbentuk $\Sigma = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$ dengan D merupakan matriks diagonal berukuran $k \times k$ yang berisi singular value dari A dengan urutan tidak turun, serta U adalah matriks ortogonal berukuran $m \times n$ dan V adalah matriks ortogonal berukuran $n \times n$. (Anton & Rorres, 2014)

Invers Matriks Diperluas (*Pseudoinvers*)

Pseudoinvers dari matriks $A \in M_{m\times n}$ dinotasikan dengan $A^{\dagger}$, yaitu matriks $X \in M_{n\times m}$ yang memenuhi 4 persamaan berikut.

$$AXA = A$$
$$XAX = X$$
$$(AX)^* = AX$$
$$(XA)^* = XA$$

dengan A^* adalah transpose kojugat dari A. (Penrose, 1955)

Teorema *Pseudoinvers*

Diberikan matriks $A \in M_{m\times n}$ maka terdapat secara tunggal matriks $B \in M_{n\times m}$ yang merupakan *pseudoinvers* dari A.

Bukti

Berdasarkan *SVD* matriks A dapat dituliskan kedalam bentuk $A = U\Sigma V^*$ sehingga diperoleh *pseudoinvers* dari matriks A adalah $A^{\dagger} = V\Sigma^{\dagger}U^*$ dengan $\Sigma^{\dagger} = \begin{bmatrix} D^{-1} & 0 \\ 0 & 0 \end{bmatrix}$. Jadi, terbukti bahwa *pseudoinvers* dari matriks A dijamin ada dengan *SVD*.

Misalkan matriks $B, C \in M_{n\times m}$ adalah *pseudoinvers* dari matriks A maka memenuhi

$$\begin{aligned} AB &= (AB)^* \\ &= \big((ACA)B\big)^* \\ &= \big((AC)(AB)\big)^* \\ &= (AB)^*(AC)^* \\ &= (AB)(AC) \\ &= (ABA)C \\ &= AC \end{aligned}$$

Sehingga jika dikalikan B pada sisi kiri pada persamaan diatas diperoleh

$$BAB = BAC$$
$$B = BAC$$

Disisi lain diperoleh juga

$$\begin{aligned} BA &= (BA)^* \\ &= (B(ACA))^* \\ &= \big((BA)(CA)\big)^* \\ &= (CA)^*(BA)^* \end{aligned}$$

$$= (CA)(BA)$$
$$= C(ABA)$$
$$= CA$$

Sehingga jika dikalikan C pada sisi kanan pada persamaan diatas diperoleh

$$BAC = CAC$$
$$BAC = C$$

Sehingga terbukti bahwa $B = C$ yang mengimplikasikan bahwa *pseudoinvers* tunggal.

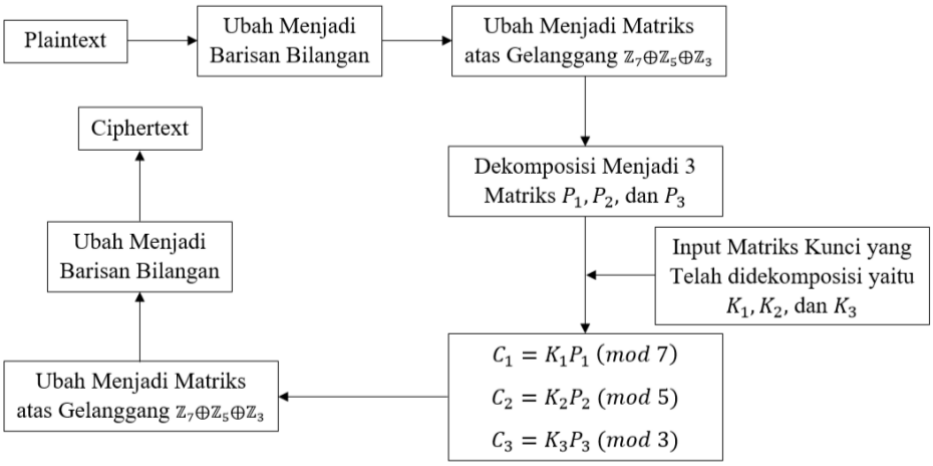
HASIL

Pada bagian ini akan dijelaskan mengenai implemetasi dari matriks atas gelanggang $\mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$ pada algoritma Cipher Hill. Tabel 3 merupakan tabel korespondensi $1-1$ dari alfabet dengan gelanggang $\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3$. $\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3$ dipilih karena 7,5, dan 3 merupakan bilangan prima sehingga invers dari matriks kunci atas gelanggang tersebut ada jika determinannya tidak nol.

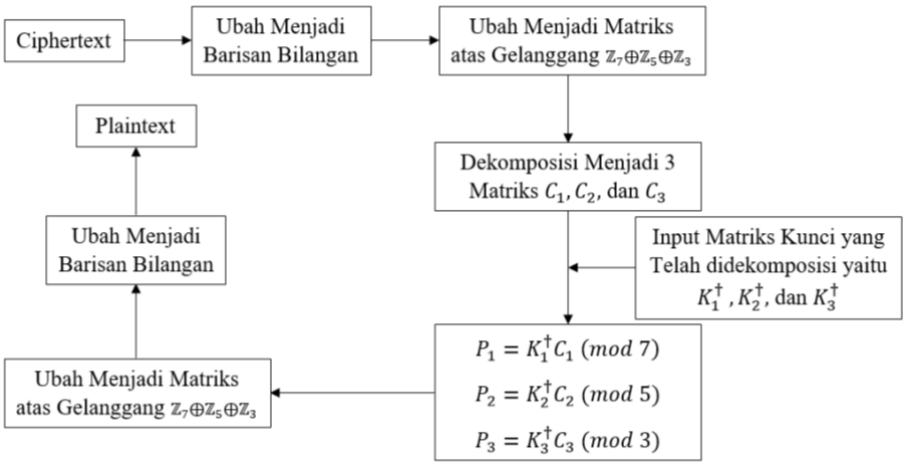
Tabel 3. Tabel pemetaan $1-1$ dari alfabet ke gelanggang $\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3$

Spasi	!	“	#	$	%	&	‘	(
(**0**, **0**, **0**)	(0,0,1)	(0,0,2)	(0,1,0)	(0,1,1)	(0,1,2)	(0,2,0)	(0,2,1)	(0,2,2)
)	*****	**+**	**,**	**-**	**.**	**/**	**0**	**1**
(**0**, **3**, **0**)	(0,3,1)	(0,3,2)	(0,4,0)	(0,4,1)	(0,4,2)	(1,0,0)	(1,0,1)	(1,0,2)
2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**:**
(**1**, **1**, **0**)	(1,1,1)	(1,1,2)	(1,2,0)	(1,2,1)	(1,2,2)	(1,3,0)	(1,3,1)	(1,3,2)
;	<	=	>	**?**	**@**	**A**	**B**	**C**
(**1**, **4**, **0**)	(1,4,1)	(1,4,2)	(2,0,0)	(2,0,1)	(2,0,2)	(2,1,0)	(2,1,1)	(2,1,2)
D	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
(**2**, **2**, **0**)	(2,2,1)	(2,2,2)	(2,3,0)	(2,3,1)	(2,3,2)	(2,4,0)	(2,4,1)	(2,4,2)
M	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**
(**3**, **0**, **0**)	(3,0,1)	(3,0,2)	(3,1,0)	(3,1,1)	(3,1,2)	(3,2,0)	(3,2,1)	(3,2,2)
V	**W**	**X**	**Y**	**Z**	**[**	\	**]**	^
(**3**, **3**, **0**)	(3,3,1)	(3,3,2)	(3,4,0)	(3,4,1)	(3,4,2)	(4,0,0)	(4,0,1)	(4,0,2)
_	**`**	**a**	**b**	**c**	**d**	**e**	**f**	**g**
(**4**, **1**, **0**)	(4,1,1)	(4,1,2)	(4,2,0)	(4,2,1)	(4,2,2)	(4,3,0)	(4,3,1)	(4,3,2)
h	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**
(**4**, **4**, **0**)	(4,4,1)	(4,4,2)	(5,0,0)	(5,0,1)	(5,0,2)	(5,1,0)	(5,1,1)	(5,1,2)
q	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**
(**5**, **2**, **0**)	(5,2,1)	(5,2,2)	(5,3,0)	(5,3,1)	(5,3,2)	(5,4,0)	(5,4,1)	(5,4,2)
z	**{**	**|**	**}**	**~**	**™**	**©**	**¬**	**®**
(**6**, **0**, **0**)	(6,0,1)	(6,0,2)	(6,1,0)	(6,1,1)	(6,1,2)	(6,2,0)	(6,2,1)	(6,2,2)
°	±	2	3	1	÷			
(**6**, **3**, **0**)	(6,3,1)	(6,3,2)	(6,4,0)	(6,4,1)	(6,4,2)			

Proses enrkipsi dan dekripsi pada perluasan algoritma Cipher Hill menggunakan matriks atas gelanggang $\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3$ akan dijelaskan melalui Gambar 3 dan Gambar 4.



Gambar 3. Skema proses enkripsi algoritma Cipher Hill menggunakan matriks atas gelanggang $\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3$



Gambar 4. Skema proses dekripsi algoritma Cipher Hill menggunakan matriks atas gelanggang $\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3$

Sebagai contoh misalkan *plaintext* "Secret." akan dienkripsi menggunakan kunci "Rahasia". Dengan menggunakan tabel 3 diperoleh barisan angka untuk *plaintext* adalah $(3,2,0), (4,3,0), (4,2,1), (5,2,1), (4,3,0), (5,3,0), (0,4,2)$ dan barisan angka untuk kata kuncinya adalah $(3,1,2), (4,1,2), (4,4,0), (4,1,2), (5,2,2), (4,4,1), (4,1,2)$. Selanjutnya dari barisan angka tersebut diubah menjadi matriks 7×1 dan 1×7 yaitu

$$P = \begin{bmatrix} (3,2,0) \\ (4,3,0) \\ (4,2,1) \\ (5,2,1) \\ (4,2,0) \\ (5,3,0) \\ (0,4,2) \end{bmatrix}$$

$$K = [(3,1,2) \quad (4,1,2) \quad (4,4,0) \quad (4,1,2) \quad (5,2,2) \quad (4,4,1) \quad (4,1,2)]$$

Sehingga diperoleh matriks dekomposisinya adalah

$$P_1 = \begin{bmatrix}3\\4\\4\\5\\4\\5\\0\end{bmatrix}, P_2 = \begin{bmatrix}2\\3\\2\\2\\2\\3\\4\end{bmatrix}, P_3 = \begin{bmatrix}0\\0\\1\\1\\0\\0\\2\end{bmatrix}$$

$$K_1 = [3 \quad 4 \quad 4 \quad 4 \quad 5 \quad 4 \quad 4], K_2 = [1 \quad 1 \quad 4 \quad 1 \quad 2 \quad 4 \quad 1], K_3 = [2 \quad 2 \quad 0 \quad 2 \quad 2 \quad 1 \quad 2]$$

dan diperoleh *ciphertext* yang terdekomposisi yaitu

$$C_1 = K_1P_1 \ (mod\ 7)$$

$$= [3 \quad 4 \quad 4 \quad 4 \quad 5 \quad 4 \quad 4]\begin{bmatrix}3\\4\\4\\5\\4\\5\\0\end{bmatrix} (mod\ 7)$$

$$= [101] \ (mod\ 7)$$

$$= [3]$$

$$C_2 = K_2P_2 \ (mod\ 5)$$

$$= [1 \quad 1 \quad 4 \quad 1 \quad 2 \quad 4 \quad 1]\begin{bmatrix}2\\3\\2\\2\\2\\3\\4\end{bmatrix} (mod\ 5)$$

$$= [35] \ (mod\ 5)$$

$$= [0]$$

$$C_3 = K_3P_3 \ (mod\ 3)$$

$$= [2 \quad 2 \quad 0 \quad 2 \quad 2 \quad 1 \quad 2]\begin{bmatrix}0\\0\\1\\1\\0\\0\\2\end{bmatrix} (mod\ 3)$$

$$= [6] \ (mod\ 3)$$

$$= [0]$$

Jadi, diperoleh matriks $C = [(3,0,0)]$ dan barisan angkanya adalah (3,0,0) yang berkorespondensi dengan huruf "M". Dengan demikian hasil enkripsi *plaintext* "Secret." dengan kunci "Rahasia" adalah "M".

PENUTUP

Matriks atas gelanggang $\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3$ dapat diimplementasikan untuk memperluas ruang kunci pada algoritma Cipher Hill sehingga proses enkripsi-dekripsi dapat bervariasi. Penerapan invers matriks diperluas juga memungkinkan adanya matriks kunci yang tak persegi untuk digunakan sebagai kunci dalam proses enkripsi-dekripsi. Dengan demikian *plaintext* dengan panjang berapapun dapat langsung di enkripsi tanpa harus menambah huruf tertentu. Selain itu, hasil enkripsi memungkinkan panjang *plaintext* akan berbeda dengan panjang dari

ciphertext. Oleh karena itu, matriks atas gelanggang $\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3$ dapat meutupi kedua kelemahan yang ada pada algoritma Cipher Hill.

DAFTAR RUJUKAN

Anton, H., & Rorres, C. (2014). *Elementary Linear Algebra* (11th ed.). John Wiley.

Brown, W. C. (1993). *Matrices Over Commutative Rings*. Marcel Dekker.

Buchmann, J. A. (2001). *Introduction to Cryptography*. Springer.

Gallian, J. A. (2021). *Contemporary Abstract Algebra* (10th ed.). CRC Press.

Hill, L. S. (1929). Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly*, *36*(6), 306–312.

Penrose, R. (1955). A generalized inverse for matrices. *Mathematical Proceedings of the Cambridge Philosophical Society, 51*(3), 406–413.

Solikhin, M., Nainggolan, S.P., & Fitriyaningsih, I.(2022). Aplikasi Invers Matriks Diperluas (Pseudoinvers) Pada Kriptografi Cipher Hill Atas Lapangan $\mathbb{Z}97$. *JKMA: Jurnal Kajian Matematika dan Aplikasinya*, 3(2), 26-32.