JKMA Jurnal Kajian Matematika dan Aplikasinya
VOLUME 3 NOMOR 2, July 2022
e-ISSN: 2722-7650. http://journal2.um.ac.id/index.php/jkma

APLIKASI INVERS MATRIKS DIPERLUAS (*PSEUDOINVERSE*) PADA KRIPTOGRAFI CIPHER HILL ATAS LAPANGAN $\mathbb{Z}_{97}$

Mukhammad Solikhin[1,*], Sahat Pandapotan Nainggolan[2], Ike Fitriyaningsih[2]
[1] Universitas Negeri Malang
[2] Faculty of Vocation, Del Institute of Technology

Email : mukhammad.solikhin.fmipa@um.ac.id (*M. Solikhin*), sahat.nainggolan@del.ac.id (*S.P. Nainggolan*), ike.fitriyaningsih@del.ac.id (*I. Fitriyaningsih*)
*****Corresponding Author

Abstract
Kriptografi adalah sebuah metode dalam mengamankan pesan dengan menggunakan algoritma matematika tertentu. Dalam kriptografi terdapat dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses merubah informasi yang dapat dimengerti maknanya menjadi informasi yang tidak dapat dimengerti artinya. Sedangkan dekripsi adalah proses sebaliknya, yaitu mengubah informasi yang tidak dipahami artinya menjadi informasi yang bermakna atau dapat dipahami maksudnya. Dalam sistem kriptografi, informasi yang dapat dimengerti artinya disebut dengan plaintext(clear text) sedangkan informasi yang tidak dapat dimengerti maknanya disebut dengan ciphertext(fuzzy text). Salah satu jenis algoritma adalah algoritma Hill atau yang biasa dikenal dengan Hill Cipher, merupakan algoritma yang menggunakan matriks persegi untuk enkripsi dan dekripsi, pada penelitian ini penulis memperluas teknik kriptografi Hill cipher tidak hanya menggunakan matriks persegi sebagai kunci tetapi juga matriks tak-persegi pada teknik kriptografi kunci simetris dengan bantuan teorema pseudoinverse, yaitu teorema yang memastikan bahwa setiap matriks tak-persegi atas field memiliki invers yang disebut matriks pseudoinverse. Penulis juga menggunakan teorema yang memudahkan dalam pencarian matriks pseudoinverse, beberapa diantaranya adalah jika matriks tersebut invertible atau memiliki rank kolom penuh atau bisa juga jika memiliki rank baris penuh, selanjutnya berdasarkan teorema tersebut, penulis juga membuat program implementasi dari perluasan kriptografi cipher Hill dengan tujuan agar dengan teorema-teorema tersebut dapat dibuat sebuah aplikasi yang dapat digunakan untuk bertukar pesan rahasia, namun ditemukan bahwa extended hill cryptographic cipher menghasilkan ciphertext yang lebih panjang dari plaintext sehingga lebih menguntungkan karena pesan menjadi semakin sulit untuk didekodekan.

***Keywords**: Cryptography, Dekripsi, Enkripsi, Hill Cipher, Pseudoinverse, Kriptografi.*

Submitted: 14 March 2022; Revised: 20 June 2022; Accepted Publication: 3 July 2022;
Published Online: July 2022
DOI: 10.17977/um055v3i2p26-32

PENDAHULUAN

Kriptografi adalah teknik atau upaya mengamankan informasi dari pihak yang dianggap tidak layak untuk mendapatkan informasi tersebut dengan menggunakan suatu algoritma tertentu. Sistem kriptografi secara umum terdiri dari dua proses, yaitu proses enkripsi dan dekripsi. Enkripsi adalah proses merubah informasi yang dapat dimengerti maknanya menjadi informasi yang tidak dapat dimengerti artinya. Sedangkan dekripsi adalah proses sebaliknya, yaitu mengubah informasi yang tidak dipahami artinya menjadi informasi yang bermakna atau dapat dipahami maksudnya. Dalam sistem kriptografi, Informasi yang dapat dimengerti artinya disebut dengan plaintext sedangkan informasi yang tidak dapat dimengerti maknanya disebut dengan ciphertext.

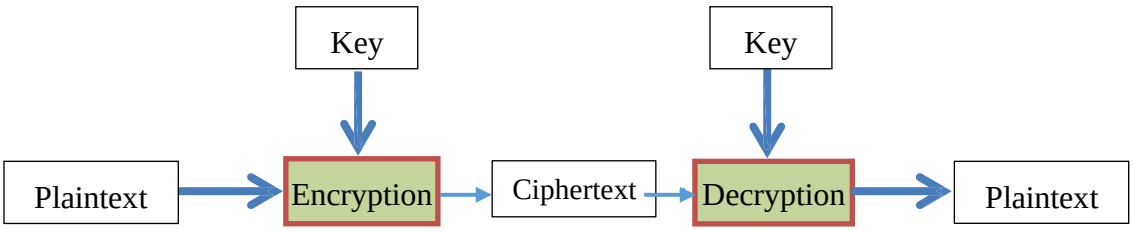
Salah satu algoritma dalam sistem kriptografi adalah algoritma Cipher Hill yang diperkenalkan pada [1,2]. Ide dasar kriptografi Cipher Hill adalah membuat korespondensi 1-1

antara huruf dengan angka atas lapangan $\mathbb{Z}_{26}$ sehingga diperoleh barisan angka yang berkorespondensi dengan huruf-huruf alfabet. Tabel 1 merupakan salah satu contoh korespondensi satu-satu dari alfabet ke dalam angka bilangan bulat anggota $\mathbb{Z}_{26}$.

Tabel 1. Contoh Pemetaan 1-1 dari Alfabet ke Dalam Lapangan $\mathbb{Z}_{26}$

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

Dalam proses enkripsi, sebuah plainteks p dirubah menjadi barisan bilangan, berdasarkan Tabel 1, kemudian disusun ke dalam bentuk matriks dan dikalikan dengan sebuah matriks invertible K sehingga manghasilkan matriks cipherteks C, sedangkan untuk mendekripsi pesan tersebut, matriks cipherteks C dikalikan dengan invers dari matriks K sehingga diperoleh kembali matriks plaintext P. Sepasang matriks invertible K dan K^{-1} yang dipilih dalam proses enkripsi-dekripsi tersebut biasa disebut sebagai matriks kunci. Gambar 1 di bawah ini adalah proses enkripsi-dekripsi menggunakan cipher Hill.



Gambar 1. Skema Sistem Kriptografi Cipher Hill

Kriptografi cipher Hill pada gambar 1 di atas memiliki beberapa kelemahan diantaranya adalah matriks kunci yang digunakan haruslah invertible yang artinya, secara tidak langsung mensyaratkan bahwa matriks kunci tersebut haruslah persegi, hal tersebut menjadi pembatas dalam pemilihan matriks sebagai matriks kunci. Kekurangan yang kedua adalah pada proses perubahan plaintext atau ciphertext dari barisan angka-angka menjadi matriks persegi, tidak selalu dapat diperoleh sebuah matriks yang tepat persegi, sebagai contoh plainteks "talking" dengan menggunakan korespondensi pada Tabel 1 berubah menjadi barisan angka "19,14,23,10,17,0,6" yang tidak dapat secara langsung diubah ke dalam bentuk matriks persegi, hal tersebut mengakibatkan proses enkripsi-dekripsi tidak dapat dilakukan secara langsung pada plaintext tersebut.

Pada penelitian ini dibahas mengenai konsep invers matriks diperluas (*pseudoinverse*) yang akan memberikan solusi atas permasalahan atau kelemahan yang ada pada sistem kriptografi cipher hill atas field $\mathbb{Z}_{26}$. Penelitian ini disusun sebegai berikut. Pada bagian 2 membahas kriptografi cipher Hill. Bagian 3 invers matriks diperluas akan dibahas lebih dalam. Aplikasi dari invers matriks diperluas juga dibahas pada bagian 4. Bagian terakhir berisi hasil dan rangkuman penelitian.

KRIPTOGRAFI CIPHER HILL

Sebuah plainteks p dengan panjang n akan dienkripsi dengan terlebih dahulu merubah plainteks tersebut menggunakan korespondensi 1-1, sehingga diperoleh barisan angka. Selanjutnya barisan angka tersebut diubah ke dalam bentuk matriks persegi dan diperoleh matriks plaintext P dengan entri bilangan bulat anggota $\mathbb{Z}_{26}$. Proses enkripsi dilanjutkan dengan mengalikan matriks plaintext P tersebut dengan matriks invertible K yang ukurannya sesuai dengan matriks plaintext P sehingga menghasilkan matriks baru yang disebut matriks ciphertext C. Selanjutnya matriks ciphertext C diubah kembali ke dalam barisan angka dan

dikorespondensikan dengan alfabet yang bersesuaian sehingga diperoleh ciphertext c. Ciphertext c ini yang kemudian akan dikirim kepada penerima sebagai pesan yang terenkripsi.

Sedangkan untuk proses dekripsi, ciphertext c dikorespondensikan kembali dengan angka-angka dan disusun ke dalam bentuk matriks persegi, sehingga diperoleh matriks ciphertext C, selanjutnya matriks ciphertext C dikalikan dengan invers dari matriks kunci K, yaitu K^{-1} dan diperoleh matriks plaintext P. Langkah selanjutnya merubah matriks plaintext P tersebut ke dalam barisan angka dan dikorespondensikan dengan alfabet yang bersesuaian sehingga diperoleh kembali plaintext p semula.

Tabel 2. Contoh Lain Pemetaan 1-1 dari Alfabet ke Dalam Lapangan $\mathbb{Z}_{26}$

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, sebuah plaintext "SECRET" berkorespondensi dengan barisan bilangan "18,4,2,17,4,19" dienkripsi dengan menggunakan matriks kunci

$$K = \begin{bmatrix} 5 & -1 \\ 9 & -2 \end{bmatrix} \tag{1}$$

akan menghasilkan ciphertext

$$C = (P.K)\ mod\ 26 \tag{2}$$

$$= \begin{bmatrix} 18 & 17 \\ 4 & 4 \\ 2 & 19 \end{bmatrix} \begin{bmatrix} 5 & -1 \\ 9 & -2 \end{bmatrix} mod\ 26 \tag{3}$$

$$= \begin{bmatrix} 243 & -52 \\ 56 & -12 \\ 181 & -40 \end{bmatrix} mod\ 26 \tag{4}$$

$$= \begin{bmatrix} 9 & 0 \\ 4 & 14 \\ 25 & 12 \end{bmatrix} \tag{5}$$

yang bersesuaian dengan kata "JEZAOM". Untuk mendekripsi ciphertext tersebut menggunakan invers dari matriks kunci K, dengan

$$K^{-1} = \begin{bmatrix} 2 & -1 \\ 9 & -5 \end{bmatrix} \tag{6}$$

dan diperoleh

$$P = (C.K^{-1})\ mod\ 26 \tag{7}$$

$$= \begin{bmatrix} 9 & 0 \\ 4 & 14 \\ 25 & 12 \end{bmatrix} \begin{bmatrix} 2 & -1 \\ 9 & -5 \end{bmatrix} mod\ 26 \tag{8}$$

$$= \begin{bmatrix} 18 & -9 \\ 134 & -74 \\ 158 & -85 \end{bmatrix} mod\ 26 \tag{9}$$

$$= \begin{bmatrix} 18 & 17 \\ 4 & 14 \\ 2 & 19 \end{bmatrix} \tag{10}$$

yang bersesuaian dengan plaintext "SECRET".

Secara matematis proses enkripsi-dekripsi dijelaskan sebagai berikut, diberikan $\mathcal{K}$ himpunan matriks-matriks invertible, $\mathcal{P}$ adalah himpunan plaintext dan $\mathcal{C}$ adalah himpunan ciphertext over field $\mathbb{Z}_n$. Cipher Hill mengambil $K \in \mathcal{K}$ over field $\mathbb{Z}_n$ berukuran $m \times m$ sebagai kunci. Sebuah plaintext x dengan panjang m,

$$x = [x_1 \quad x_2 \quad \dots \quad x_m] \in \mathcal{P}$$

akan dienkripsi menjadi ciphertext $y = [y_1 \quad y_2 \quad \cdots \quad y_m] \in \mathcal{C}$ dengan menggunakan matriks kunci K melalui persamaan

$$y = Kx \bmod n$$

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{14} \\ k_{21} & k_{22} & \dots & k_{24} \\ \vdots & \vdots & \ddots & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} \bmod n$$

sedangkan untuk proses dekripsi ciphertext y menjadi plaintext x adalah dengan mengalikan invers dari K

$$\begin{aligned} y &= (Kx) \bmod n \\ K^{-1}(y) \bmod n &= K^{-1}(Kx) \bmod n \\ (K^{-1}y) \bmod n &= (K^{-1}K)x \bmod n \\ (K^{-1}y) \bmod n &= x. \end{aligned}$$

HASIL DAN PEMBAHASAN

Berikut di bawah ini akan dibahas eksistensi dan ketunggalan dari invers matris diperluas (Pseudoinvers) dalam pembuatan sistem kriptografi diperluas menggunakan teorema *Singular Value Decomposition(SVD).*

Invers Matriks Diperluas(*Pseudoinverses)*

Pseudoinverse dari $A \in H^{m\times n}$, dinotasikan dengan $A^{\dagger}$, adalah matriks unik $X \in H^{n\times m}$ yang memenuhi empat persamaan berikut

$$\begin{aligned} AXA &= A \\ XAX &= X \\ (AX)^* &= AX \\ (XA)^* &= XA \end{aligned}$$

dengan A^* adalah transpose konjugat dari A.

Teorema Pseudoinverse

Diberikan A sebarang matriks berukuran $m \times n$ atas suatu lapangan maka terdapat dengan tunggal matriks *B* berukuran $n \times m$ pseudoinverse dari A.

Bukti

Untuk ketunggalan, misal X dan Y adalah Moore-Penrose inverse dari A maka X dan Y memenuhi TEO A sehingga AY, AX, XA dan YA adalah matriks hermit akibatnya

$$\begin{aligned} AY &= (\mathrm{AY})^* & YA &= (\mathrm{YA})^* \\ &= ((\mathrm{AXA})\,\mathrm{Y})^* & &= (\mathrm{Y}(\mathrm{AXA}))^* \\ &= ((\mathrm{AX})(\mathrm{AY}))^* & &= ((\mathrm{YA})(\mathrm{XA}))^* \\ &= (\mathrm{AY})^*(\mathrm{AX})^* & &= (\mathrm{XA})^*(\mathrm{YA})^* \\ &= (\mathrm{AY})(\mathrm{AX}) & &= (\mathrm{XA})(\mathrm{YA}) \\ &= (\mathrm{AYA})\,\mathrm{X} & &= \mathrm{X}(\mathrm{AYA}) \\ &= \mathrm{AX} & &= \mathrm{XA} \end{aligned}$$

$$\begin{aligned} AY &= AX & YA &= XA \\ \mathrm{Y}(\mathrm{AY}) &= \mathrm{Y}(\mathrm{AX}) & (\mathrm{YA})\,\mathrm{X} &= (\mathrm{XA})\,\mathrm{X} \\ \mathrm{YAY} &= \mathrm{YAX} & \mathrm{YAX} &= \mathrm{XAX} \\ \mathrm{Y} &= \mathrm{YAX} & \mathrm{YAX} &= \mathrm{X} \end{aligned}$$

Sehingga $Y = X$

Untuk Eksistensi, terbukti menggunakan TEO SVD.

Teorema Singular Value Decomposition

Misalkan A adalah matriks m × n dengan rank r. Maka terdapat Σ matriks m × n dengan $\Sigma = \begin{bmatrix} \mathrm{D} & 0 \\ 0 & 0 \end{bmatrix}$ dengan entri diagonal matriks D adalah r nilai singular dari A, $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r > 0$, dan terdapat matriks ortogonal U m × m dan matriks ortogonal V n × n sehingga $A = U\Sigma V^T$.

Lemma

Jika A invertibel, maka $A^{\dagger} = A^{-1}$.
Jika A mempunyai invers kanan R, ($AR = I_m$), maka $A^{\dagger} = R$.
Jika A mempunyai invers kiri L, ($LA = I_n$), maka $A^{\dagger} = L$.
Jika A mempunyai rank kolom penuh (*full column rank)*, maka $A^{\dagger} = (A^*A)^{-1}A^*$
Jika A mempunyai rank baris penuh (*full row rank)*, maka $A^{\dagger} = A^*(AA^*)^{-1}$

$$\left(A^{\dagger}\right)^{\dagger} = A$$
$$(A^*)^{\dagger} = \left(A^{\dagger}\right)^*.$$

HASIL

Tabel 3 merupakan korespondensi 1-1 dari huruf ke angka bilangan bulat modulo 97, $\mathbb{Z}_{97}$ dipilih karena 97 adalah bilangan prima akibatnya berdasarkan [] setiap elemen tak nolnya memiliki invers, sehingga dapat menjamin setiap matriks kunci yang memiliki determinan tak nol yang akan dipilih selalu memiliki invers di modulo $\mathbb{Z}_{97}$. Misalkan diberikan tabel korespondensi 1-1 dari abjad ke bilangan bulat modulo 97 seperti dalam Tabel 3 berikut ini.

Tabel 3. Konversi Huruf dan Angka pada bilangan bulat modulo 97

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
0	1	2	3	4	5	6	7	8	9	10	11	12	13
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**a**	**b**
14	15	16	17	18	19	20	21	22	23	24	25	26	27
c	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**
28	29	30	31	32	33	34	35	36	37	38	39	40	41
q	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**{**	**|**	**}**	**~**
42	43	44	45	46	47	48	49	50	51	52	53	54	55
space	**!**	**“**	**#**	**$**	**%**	**&**	**‘**	**(**	**)**	*****	**+**	**,**	**-**
56	57	58	59	60	61	62	63	64	65	66	67	68	69
.	**/**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**:**	**;**
70	71	72	73	74	75	76	77	78	79	80	81	82	83
<	**=**	**>**	**?**	**@**	**[**	****	**]**	**^**	**_**	**¼**	**½**	**¾**	
84	85	86	87	88	89	90	91	92	93	94	95	96	

Misalkan plaintext $P_1 =$ T@Lk! nG akan dienkripsi menggunakan kunci $K_1 =$ \$3cRet. yang berdasarkan Tabel 3 berturut-turut berkorespondensi dengan barisan bilangan “19,88,11,36,57,39,6” dan “60,75,28,17,30,45,70” memiliki matriks plaintext dan kunci berturut-turut sebagai

$$P_1 = \begin{bmatrix} 19 \\ 88 \\ 11 \\ 36 \\ 57 \\ 39 \\ 6 \end{bmatrix}, K_1 = [60 \quad 75 \quad 28 \quad 17 \quad 30 \quad 45 \quad 70]$$

Ciphertext C_1 diperoleh dengan

$$C_1 = (K_1P_1)\ mod\ 97$$
$$= [60 \quad 75 \quad 28 \quad 17 \quad 30 \quad 45 \quad 70] \begin{bmatrix} 19 \\ 88 \\ 11 \\ 36 \\ 57 \\ 39 \\ 6 \end{bmatrix} mod\ 97$$

$$= [12545] \; mod \; 97 = 32.$$

Sehingga berdasarkan Tabel 3 diperoleh plainteks $P_1 =$ T@Lk! nG dienkripsi dengan kunci K_1 menjadi ciphertext $C_1 = g$.

Apabila matriks plaintext P dan matriks kunci K dirubah ukuran matriksnya maka akan diperoleh ciphertext yang berbeda. Sebagai contoh plaintext dan matriks kunci di atas di rubah ke dalam bentuk

$$P_2 = [19 \quad 88 \quad 11 \quad 36 \quad 57 \quad 39 \quad 6], \; K_2 = \begin{bmatrix} 60 \\ 75 \\ 28 \\ 17 \\ 30 \\ 45 \\ 70 \end{bmatrix}$$

Maka diperoleh matriks ciphertext C_2 sebagai berikut

$$C_2 = (K_2 P_2) \; mod \; 97$$

$$= \begin{bmatrix} 60 \\ 75 \\ 28 \\ 17 \\ 30 \\ 45 \\ 70 \end{bmatrix} [19 \quad 88 \quad 11 \quad 36 \quad 57 \quad 39 \quad 6] \; mod \; 97$$

$$= \begin{bmatrix} 73 & 42 & 78 & 26 & 25 & 12 & 69 \\ 67 & 4 & 49 & 81 & 7 & 15 & 62 \\ 47 & 39 & 17 & 38 & 44 & 25 & 71 \\ 32 & 41 & 90 & 30 & 96 & 81 & 5 \\ 85 & 21 & 39 & 13 & 61 & 6 & 83 \\ 79 & 80 & 10 & 68 & 43 & 9 & 76 \\ 69 & 49 & 91 & 95 & 13 & 14 & 32 \end{bmatrix}$$

Dengan menggunakan Tabel 3 diperoleh plainteks $P_2 =$ T@Lk! nG dienkripsi dengan kunci K_2 menjadi ciphertext $C_2 =$ "1 + vg = 7 − qEnpV8x6xR\nK]a9meN, ½ZHs¾%rNMPZ9GJO − &/F; 4g".

PENUTUP

Konsep invers matriks diperluas dapat diterapkan untuk memperluas sistem kriptografi cipher hill di bilangan bulat modulo 26 menjadi bilangan bulat modulo 97, selain itu dengan konsep tersebut, pemilihan matriks kunci untuk proses enkripsi-dekripsi menjadi lebih bervariatif karena tidak mengharuskan menggunakan matriks persegi sebagai matriks kunci, matriks tak persegi, asal memenuhi sifat-sifat tertentu juga dapat digunakan sebagai matriks kunci untuk proses enkripsi-dekripsi. Penerapan konsep invers matriks diperluas pada kriptografi cipher hill juga dapat mengenkripsi secara simultan plaintext menjadi ciphertext ataupun sebaliknya tanpa harus mengubah plaintext tersebut ke dalam bentuk matriks persegi, kelebihan lainnya adalah, dengan menggunakan invers matriks tak-persegi dan merubah matriks plainteks dan matriks kunci menjadi tak-persegi membuat ciphertext yang dihasilkan semakin sulit untuk dipecahkan karena panjang ciphertext yang dihasilkan akan memiliki panjang yang berbeda sekali dengan panjang plaintext semula, sehingga semakin memperkuat sistem kriptografi dari hacking.

DAFTAR RUJUKAN

Hill, L.S. (1929). Cryptography in Algrebaist Alphabet. *American Mathematical Monthly*, 36, 306-312.

Hill, L.S. (1931). Concerning Certain Linear Transformation Apparatus of Cryptography. *American Mathematical Monthly*, 38, 135-154.

Penrose, R. (1955). A Generalized Inverse for Matrices. *Cambridge, 51,* 406-413.

Goldberg, J.L. (1991). Matrix Theory with Application. *McGraw-Hill Inc.*

Lay , D.C. (2012). Linear Algebra and Its Applications. *Addison-Wesley, 4ed.*.