MIMS Majalah Ilmiah Matematika dan Statistika 23 (2), 2023, 106 – 115
eISSN 2722-9886 pISSN 1411-6669
https://jurnal.unej.ac.id/index.php/MIMS/index

Modifikasi algoritma Hill cipher dengan matriks kunci berupa matriks ketetanggaan

(Modification of Hill cipher algorithm with key matrix in the form of a adjacency matrix)

Fakhry Asad Agusfrianto, Lukita Ambarwati, Yudi Mahatma*

Program Studi Matematika, Fakultas MIPA, Universitas Negeri Jakarta
Jakarta Timur, Jakarta 13220, Indonesia

*korespondensi: yudi_mahatma@unj.ac.id

Received: 16-12-2022, accepted: 24-07-2023

Abstract

Cryptography is one of the parts in mathematics, especially applied mathematics. Cryptography is the science that studies how to secure information that we don't want others to know about the information we have. Based on the development of the times, cryptography is divided into two consisting of classical cryptography and modern cryptography. In this paper, the focus of discussion is on classical cryptography. Furthermore, there are many kinds of classical cryptographic algorithms, such as the Caesar cipher algorithm, the Playfair cipher algorithm, the Vigenere cipher algorithm, and the Hill Cipher algorithm. The focus of discussion in this paper is on the Hill cipher algorithm. The modifications made to the Hill cipher algorithm lie in its key matrix. In this paper, it will be shown how to encrypt and decrypt the message we want to send using the Hill cipher algorithm with the matrix being a adjacency matrix. In which case, the adjacency matrix itself is obtained from the representation of the graph. It is hoped that this algorithm can avoid crypt attacks, especially on ciphertext only-attack.

Keywords: Hill cipher algorithm, cryptography, adjacency matrix, plaintext, ciphertext
MSC2020: 94A60

1. Pendahuluan

Ketika seseorang ingin mengirim pesan yang sangat penting ke seseorang lainnya, tentu mereka tidak ingin pihak ketiga selain mereka dan teman mereka mengetahui. Untuk mengatasi hal tersebut, dapat dilakukan pemodifikasian pada pesan yang ingin dikirim ke pihak lain supaya hanya pemilik pesan penerima pesan yang mengetahui makna pesan tersebut. Dalam matematika, khususnya pada matematika terapan, ilmu yang mempelajari hal tersebut dinamakan kriptografi. Kriptografi merupakan ilmu yang mempelajari terkait bagaimana mengamankan pesan menggunakan kode-kode rahasia [1]. Dalam kriptografi, terdapat istilah enkripsi, dekripsi, *plaintext*, dan *ciphertext*. Untuk penjelasan istilah

tersebut, dapat merujuk ke [1]. Berdasarkan perkembangan zaman, kriptografi terdiri atas kriptografi klasik dan kriptografi modern [2].

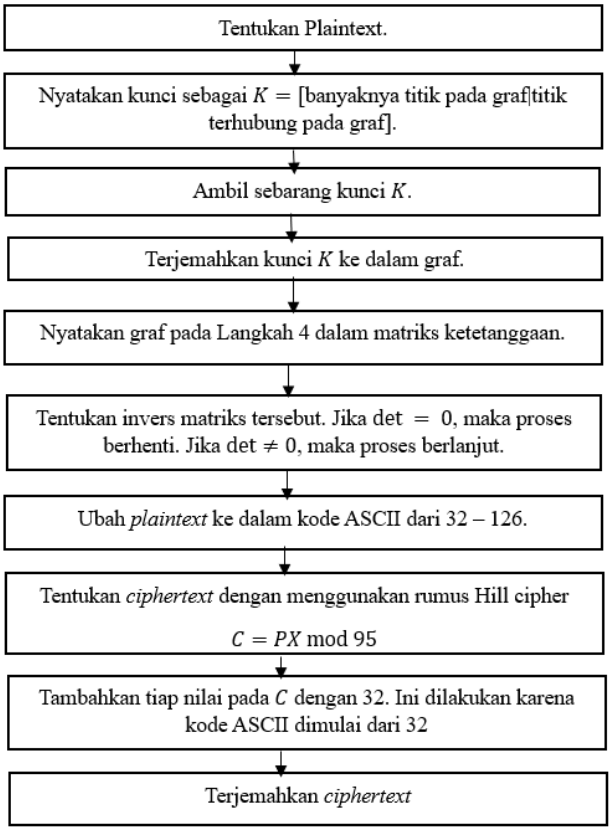
Dalam paper ini, pembahasan akan berfokus pada kriptografi klasik. Algoritma-algoritma kriptografi klasik terdiri atas berbagai macam. Algoritma tersebut antara lain adalah Caesar *cipher*, Playfair *cipher*, Vigenere *cipher*, dan Hill *cipher* [3]. Pembahasan paper ini akan berfokus pada algoritma Hill *Cipher* dan modifikasinya. Algoritma Hill cipher merupakan algoritma yang menggunakan matriks persegi sebagai kuncinya. Beberapa modifikasi yang dilakukan pada algoritma Hill *cipher* antara lain algoritma Hill *Cipher* dengan matriks kunci adalah matriks Fibonacci [4], algoritma Hill *cipher* dengan menggunakan fungsi himpunan fuzzy [5], algoritma Hill *cipher* dengan menggunakan matriks kunci persegi panjang [6], algoritma Hill *cipher* dengan pemanfaatan kunjungan pohon biner [7], algoritma Hill *cipher* dengan matriks kunci yang dibangun dari algoritma Playfair *cipher* [8], algoritma Hill *cipher* dengan menggunakan matriks sirkulan [9], algoritma Hill *cipher* dengan menggunakan tabel periodik unsur kimia [10], algoritma Hill *cipher* dengan menggunakan transposisi dan operasi XOR [11], algoritma Hill *cipher* dengan menggunakan satuan massa [12], modifikasi Hill *cipher* dengan fungsi XOR dan XNOR [13], dan Hill *cipher* untuk pengamanan fungsi hash [14].

Selanjutnya, dalam matematika terapan dikenal konsep graf. Graf merupakan himpunan yang terdiri atas titik dan sisi [15], [16]. Selanjutnya, untuk merepresentasikan banyaknya titik yang terhubung pada graf, salah satunya dapat menggunakan matriks ketetanggaan [15], [17].

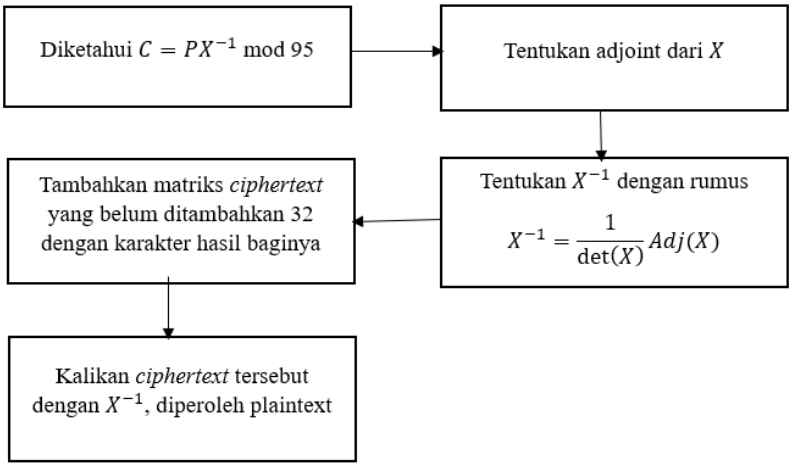
Tujuan penelitian pada paper ini adalah akan dilakukan modifikasi pada algoritma Hill *Cipher* dengan matriks kuncinya adalah matriks ketetanggaan. Karakter-karakter yang akan digunakan pada informasi yang akan dienkripsi dan didekripsi menggunakan algoritma ini adalah karakter pada tabel ASCII mulai dari karakter ke 32 sampai dengan karakter ke 126 atau total sebanyak 95 karakter. Harapan dari algoritma ini adalah dapat menghindari serangan kriptanalis yaitu *ciphertext only-attack* [1].

2. Metodologi

Metodologi yang akan digunakan pada penelitian ini adalah kajian literatur. Langkah-langkah penelitian dalam paper ini disajikan dalam diagram proses penelitian berikut.



Gambar 1. Diagram proses penelitian pengenkripsian pesan



Gambar 2. Diagram proses penelitian pendekripsian pesan

3. Hasil dan Pembahasan

Pada bagian ini, akan diberikan contoh sebarang *plaintext* yang akan dienkripsi dan didekripsi. Langkah-langkah untuk melakukan pengenkripsian dan pendekripsian adalah sebagai berikut.

3.1 Pengenkripsian Pesan

Langkah 1:

Diketahui ***plaintext*: faya tahu**. Tentukan kunci yang ingin digunakan dan nyatakan kunci sebagai

$$K = [\text{banyaknya titik pada graf}|\text{titik yang terhubung pada graf}].$$

Langkah 2:

Untuk kesepakatan penulisan, perhatikan Tabel 1.

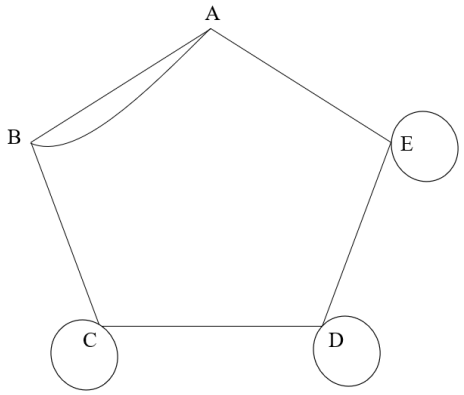
Tabel 1. Tabel penulisan kunci

Simbol	Makna
ABE	Titik A terhubung dengan titik B dan E
A^nB	Titik A terhubung-n kali dengan B
$\underline{A}$	Titik A memiliki loop

Misalkan diambil kunci $K = \left[5|A^2BE, B^2A\underline{C}, \underline{C}B\underline{D}, \underline{DCE}, \underline{E}A\underline{D}\right]$

Langkah 3:

Terjemahkan kunci tersebut ke dalam graf. Diperoleh gambar graf sebagai berikut.



Gambar 3. Graf dari kunci K

Langkah 4:

Nyatakan graf pada Gambar 1 dalam matriks ketetanggaan. Matriks ketetanggaan adalah matriks yang menyatakan keterhubungan titik suatu graf [15]. Matriks ketetanggaan dari graf diatas adalah

$$X = \begin{bmatrix} 0 & 2 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Langkah 5**:**

Karena akan digunakan invers matriks untuk melakukan dekripsi pesan, maka harus dicek apakah $(X) \neq 0$. Jika $det\ (X) = 0$, maka proses berhenti dan harus ditentukan jenis graf yang lain. Dalam kasus ini, diperoleh $det\ (X) = 9$.

Langkah 6:

Setelah itu, Ubah *plaintext* **faya tahu** ke dalam kode ASCII pada Tabel 2.

Tabel 2. Tabel ASCII

Desimal	Karakter	Desimal	Karakter	Desimal	Karakter	Desimal	Karakter	Desimal	Karakter
32	spasi	51	3	70	F	89	Y	108	l
33	!	52	4	71	G	90	Z	109	m
34	“	53	5	72	H	91	[	110	n
35	#	54	6	73	I	92	\	111	o
36	$	55	7	74	J	93	]	112	p
37	%	56	8	75	K	94	^	113	q
38	&	57	9	76	L	95	_	114	r
39	‘	58	:	77	M	96	’	115	s
40	(	59	;	78	N	97	a	116	t
41	)	60	<	79	O	98	b	117	u
42	*	61	=	80	P	99	c	118	v
43	+	62	>	81	Q	100	d	119	w
44	,	63	?	82	R	101	e	120	x
45	-	64	@	83	S	102	f	121	y
46	.	65	A	84	T	103	g	122	z
47	/	66	B	85	U	104	h	123	{
48	0	67	C	86	V	105	i	124	|
49	1	68	D	87	W	106	j	125	}
50	2	69	E	88	X	107	k	126	~

Karena diambil 5 titik, maka karakter dibuat menjadi masing-masing 5 karakter yaitu **faya(spasi)tahu(spasi)**. Maka diperoleh kata **faya tahu** dalam kode ASCII sebagai berikut:

faya(spasi) $= [102\ 97\ 121\ 97\ 32\ ] = P_1$,

tahu(spasi) $= [116\ 97\ 104\ 117\ 32\ ] = P_2$.

Di sini, 102 adalah kode ASCII dari f, 97 adalah kode ASCII dari a, dan seterusnya.

Langkah 7:

Tentukan *ciphertext* dengan menggunakan algoritma Hill *cipher*:

$$C = PX \; mod \; 95$$

dengan P adalah matriks *plaintext*, C adalah matriks *ciphertext*, dan X adalah matriks kunci. Dengan mensubstitusi nilai P dan Y, diperoleh rumusan:

$$C_1 = P_1 \; X \bmod 95$$

$$C_1 = \begin{bmatrix} 102 & 97 & 121 & 97 & 32 \end{bmatrix} \begin{bmatrix} 0 & 2 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} \bmod 95$$

$$C_2 = P_2 \; X \bmod 95$$

$$C_2 = \begin{bmatrix} 116 & 97 & 104 & 117 & 32 \end{bmatrix} \begin{bmatrix} 0 & 2 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} \bmod 95$$

Setelah dilakukan perhitungan, diperoleh

$$C_1 = [36_2 \; 40_3 \; 30_3 \; 60_2 \; 41_2 \;],$$
$$C_2 = [36_2 \; 51_3 \; 33_3 \; 63_2 \; 75_2 \;],$$

dengan C_1 adalah *ciphertext* dari P_1 dan C_2 adalah *ciphertext* dari P_2. Indeks pada tiap nilai adalah karakter hasil bagi dengan 95. Jika hasil bagi 0 ditulis 0, hasil bagi 1 ditulis 1, dan seterusnya.

Langkah 8:

Karena karakter dimulai dari karakter ke-32, maka tambahkan tiap nilai pada matriks C_1 dan C_2 dengan 32, diperoleh

$$C_1 = [68_2 \; 72_3 \; 62_3 \; 92_2 \; 73_2 \;],$$
$$C_2 = [68_2 \; 83_3 \; 65_3 \; 95_2 \; 107_2 \;].$$

Langkah 9:

Terjemahkan *ciphertext* yang terdapat pada Langkah 8 menjadi karakter ASCII. Bilangan desimal 68 bersesuaian dengan D, bilangan desimal 72 bersesuaian dengan karakter H, dan seterusnya. Jadi, *ciphertext* dari *plaintext* faya tahu adalah DH>]IDSA_k.

3.2 Langkah Pendekripsian Pesan

Setelah pesan dikirim dan diterima oleh penerima, maka penerima harus melakukan dekripsi pesan. Berdasarkan Langkah 8 pada langkah pengenkripsian pesan, diketahui rumusan untuk memperoleh *ciphertext* adalah

$$C = PX \bmod 95$$

maka, untuk memperoleh *plaintext* dapat menggunakan rumusan:

$$P = CX^{-1}\ mod\ 95.$$

Dalam Langkah 5 pengenkripsian pesan, telah diperoleh bahwa $det\ det\ (X) \neq 0$ yang berarti matriks X punya invers. Untuk lebih jelasnya, akan ditulis dalam bentuk langkah-langkah seperti proses mengenkripsi pesan.

Langkah 1:

Tentukan adjoint dari matriks $X = \begin{bmatrix} 0 & 2 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}$. Diperoleh adjoint dari matriks X adalah

$$\text{Adjoint}(X) = \begin{bmatrix} 0 & 3 & 0 & -3 & 3 \\ 3 & 0 & 3 & -3 & 0 \\ 0 & 3 & 0 & 6 & -6 \\ -3 & -3 & 6 & -3 & 6 \\ 3 & 0 & -6 & 6 & 0 \end{bmatrix}.$$

Langkah 2:

Tentukan invers dari X. Untuk mencari invers dari matriks X, dapat menggunakan rumus:

$$X^{-1} = \frac{1}{\det(X)}\ \text{Adjoint}(X).$$

Telah diketahui bahwa $det\ (X) = 9$. Dengan demikian diperoleh

$$X^{-1} = \begin{bmatrix} 0 & \frac{1}{3} & 0 & -\frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 & \frac{1}{3} & -\frac{1}{3} & 0 \\ 0 & \frac{1}{3} & 0 & \frac{2}{3} & -\frac{2}{3} \\ -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & 0 & -\frac{2}{3} & \frac{2}{3} & 0 \end{bmatrix}.$$

Langkah 3:

Tambahkan matriks *ciphertext* yang **belum ditambahkan 32** dengan karakter hasil baginya. Jika hasil bagi 0 ditambah 0, hasil bagi 1 ditambah 95, hasil bagi 2 ditambah 190, hasil bagi 3 ditambah 285, dan seterusnya. Notasikan matriks ini dengan D_1 untuk *ciphertext* C_1 dan D_2 untuk *ciphertext* D_2. Maka diperoleh

$$D_1 = [226\ 325\ 315\ 250\ 231\ ],$$

$$D_2 = [226\ 336\ 318\ 253\ 265\ ].$$

Langkah 4:

Kalikan D_1 dan D_2 masing-masing dengan X^{-1}. Dengan demikian, diperoleh *plaintext*

$$P_1 = [102\ 97\ 121\ 97\ 32\ ],$$

$$P_2 = [116\ 97\ 104\ 117\ 32\ ].$$

Jika P_1 dan P_2 diterjemahkan ke dalam karakter ASCII, maka diperoleh *plaintext* yang sama dengan yang diberikan di awal yaitu **faya tahu**.

3.3 Analisis Ketahanan Terhadap *Ciphertext Only-Attack*

Pada bagian ini, dianalisis ketahanan kriptografi terhadap serangan *ciphertext only-attack*. Umumnya, kunci dari algoritma Hill *cipher* dituliskan dalam bentuk

$$K = [k_{ij}].$$

Jika terjadi kebocoran beberapa *ciphertext* dan kunci, maka dengan mudah seorang kriptanalis dapat menjebol *ciphertext* tersebut. Namun, dalam penelitian ini, penulisan kunci dilakukan dengan cara yang tidak umum, yaitu

$$K = [\text{banyaknya titik pada graf}|\text{titik yang terhubung pada graf}].$$

Sebagai contoh, dari pembahasan diatas dipunyai kunci

$$K = [5|A^2BE, B^2A\underline{C}, \underline{C}B\underline{D}, \underline{DCE}, \underline{E}A\underline{D}].$$

Penulisan kunci seperti ini tidak umum seperti penulisan kunci pada algoritma Hill *cipher*. Dengan penulisan kunci seperti ini, jika terjadi kebocoran beberapa *ciphertext* dan kunci, maka kriptanalis mengalami kesulitan untuk memecahkan kunci tersebut karena penulisan kunci yang tidak umum.

4. Kesimpulan

Berdasarkan pemaparan, telah diperoleh bagaimana cara melakukan enkripsi dan dekripsi pesan dengan menggunakan modifikasi algoritma Hill *cipher* dengan matriks kuncinya adalah matriks ketetanggaan. Karena penulisan kunci dari pesan dinyatakan dalam bentuk yang tidak umum, hal ini akan mempersulit kriptanalis untuk melakukan pembobolan pesan. Untuk penelitian selanjutnya, dapat digunakan matriks Laplacian yang diperoleh dari matriks derajat dikurangi matriks ketetanggaan sebagai matriks kuncinya.

Daftar Pustaka

[1] R. Munir, *Kriptografi*, 1st ed. Penerbit Informatika, 2019.

[2] H. Delfs and H. Knelb, *Introduction to Cryptography*, 2nd ed. Springer, 2007. [Online].

[3] F. Piper and S. Murphy, *Cryptography : A Very Short Introduction*. Oxford University Press, 2002.

[4] H. Fitroti, M. U. Romdhini, and N. W. Switrayni, "Hill Cipher algorithm with generalized Fibonacci matrix in message encoding," *Eig. Math. J.*, vol. 4, no. 2, pp. 52–59, 2021.

[5] P. Noviyanti and D. Ariyus, "Modifikasi metode Hill cipher menggunakan fungsi *fuzzy* dan kode ASCII," *JurTI (Jurnal Teknol. Informasi)*, vol. 4, no. 2, pp. 174–181, 2020.

[6] A. Hidayat and T. Alawiyah, "Enkripsi dan dekripsi teks menggunakan algoritma Hill Cipher dengan kunci matriks persegi panjang," *J. Mat. Integr.*, vol. 9, no. 1, pp. 39–51, 2013. [CrossRef]

[7] T. Alawiyah, "Pemanfaatan kunjungan pohon biner pada kriptografi Hill cipher kunci matriks persegi panjang," *Indones. J. Comput. Inf. Technol.*, vol. 2, no. 1, pp. 77–82, 2017. [CrossRef]

[8] T. Alawiyah, A. B. Hikmah, W. Wiguna, M. Kusmira, H. Sutisna, and B. K. Simpony, "Generation of rectangular matrix key for Hill cipher algorithm using playfair cipher," *J. Phys. Conf. Ser.*, vol. 1641, no. 1, pp. 1–5, 2020. [CrossRef]

[9] K.A. Reddy, B. Vishnuvardhan, Madhuviswanatham, and A.V.N. Krishna, "A modified Hill cipher based on circulant matrices," *Procedia Technol.*, vol. 4, no. 1, pp. 114–118, 2012. [CrossRef]

[10] N. D. Sari and D. Arius, "Modifikasi algoritma Hill cipher dengan tabel periodik unsur kimia menggunakan kode nomor operator seluler di Indonesia," *J. Teknol. Inf.*, vol. 4, no. 2, pp. 202–207, 2020. [CrossRef]

[11] E. Y. Sari, A. R. Harir, and D. Ariyus, "Modifikasi Hill cipher mod 36 kombinasi transposisi dan XOR kunci tabel periodik dengan LSB untuk penyembunyian pesan," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 5, no. 1, p. 38, 2020,. [CrossRef]

[12] V. S. Ginting, "Penerapan algoritma Vigenere cipher dan Hill cipher menggunakan satuan massa," *J. Teknol. Inf.*, vol. 4, no. 2, pp. 241–246, 2020. [CrossRef]

[13] T. Alawiyah and A. B. Hikmah, "Modifikasi kriptografi Hill cipher kunci matriks persegi panjang menggunakan fungsi XOR dan fungsi XNOR," *Indones. J. Comput. Inf. Technol.*, vol. 1, no. 1, pp. 68–82, 2016. [CrossRef]

[14] Z. Panjaitan, E. F. Ginting, and Y. Yusnidah, "Modifikasi SHA-256 dengan algoritma Hill cipher untuk pengamanan fungsi hash dari upaya decode hash," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 19, no. 1, p. 53, 2020. [CrossRef]

[15] R. Munir, *Matematika Diskrit*, 7th ed. Penerbit Informatika, 2017.

[16] R. Diestel, *Graph Theory*. Springer, 2017.

[17] R. Bronson, G. B. Costa, and J. T. Saccoman, *Linear Algebra : Algorithms, Applications, and Techniques*. Academic Press, 2014.