Generation of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher

Generation of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher

Tuti Alawiyah[1]*, Agung Baitul Hikmah[1], Wildan Wiguna[1], Mira Kusmira[2], Herlan Sutisna[1], and Bambang Kelana Simpony[1]

[1]Sistem Informasi Kampus Kota Tasikmalaya, Universitas Bina Sarana Informatika, Tasikmalaya, Jawa Barat, Indonesia
[2]Sistem Informasi, STMIK Nusa Mandiri, Jakarta, Indonesia

E-mail: tuti.tah@bsi.ac.id

Abstract. Hill cipher is a cryptographic algorithm that uses matrix as a key by utilizing modulo operations. The key matrix used is usually made randomly as a square matrix. In this study, a key matrix was created using the Playfair Cipher algorithm as a rectangular matrix. The use of the Playfair Cipher algorithm makes it easy for users to remember key matrices, while remaining safe when distributed. Beside the key matrix security, use of a rectangular key matrix produces a longer and more complicated ciphertext to find the linear equation.

1. Introduction

Current technology makes it easy for us to exchange data, but this is also accompanied by the ease of others to access / retrieve data exchanged. Therefore, the need for effective data security is a must to protect the data being exchanged. Cryptography is widely used to protect data so that it cannot be read by other parties.

Various cryptographic algorithms have been developed at this time, one of which is hill cipher cryptography. The hill cipher cryptographic algorithm uses matrix and modulo operations to produce ciphertext that is difficult and difficult to solve by cryptanalysts. The use of matrix keys in hill cipher cryptography continues to grow. Various techniques are used in determining key matrix to improve data security systems in this algorithm. Alawiyah (2017) proposed a binary tree visit operation inserted at the beginning of the encryption process, as well as the use of a rectangular matrix key. The resulting ciphertext is complicated enough to be solved by cryptanalysts because it is difficult to find the linear equation [1].

In the other research has been proposed combines Elliptic Curve Cryptosystem with Hill Cipher (ECCHC) for image encryption technique [2]. Also there are a research for applying matrix shared as a secret key and a non-singular matrix G is used as a public key [3].

Determination and key secrecy in cryptography is very important, according to Kerckhoffs's principle that the cipher method "must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience" [4].

Ashraf have proposed modifying the hill cipher algorithm using three stages. Each stage is considered a block cipher with a block length of 128 bits and a key length of 256 bits. The key is taken from a random number generator and provides better security [5]. In Mahendra's research, the determination of key matrix is made using the playfair cipher. But the matrix

made is a square matrix. This is unique and innovative because it facilitates the determination of key matrix that play an important role in the encryption process and the description process of Hill Cipher [6].

In this research, playfair cipher will be used to determine the rectangular matrix key. Based on the results of research hidayat, the use of rectangular matrix key is safer than square matrix, because the ciphertext produced is longer than the plaintext, making it difficult for cryptanalyst to find their linear equations [7].

2. Method

The key matrix used in hill cipher cryptography is an inverse matrix. In this study the key matrix that will be used is a rectangular matrix which must have an pseudo-inverse. If the key matrix determination is usually made randomly, then in this study the key matrix will be obtained from the ciphertext generated from the playfair cipher algorithm.

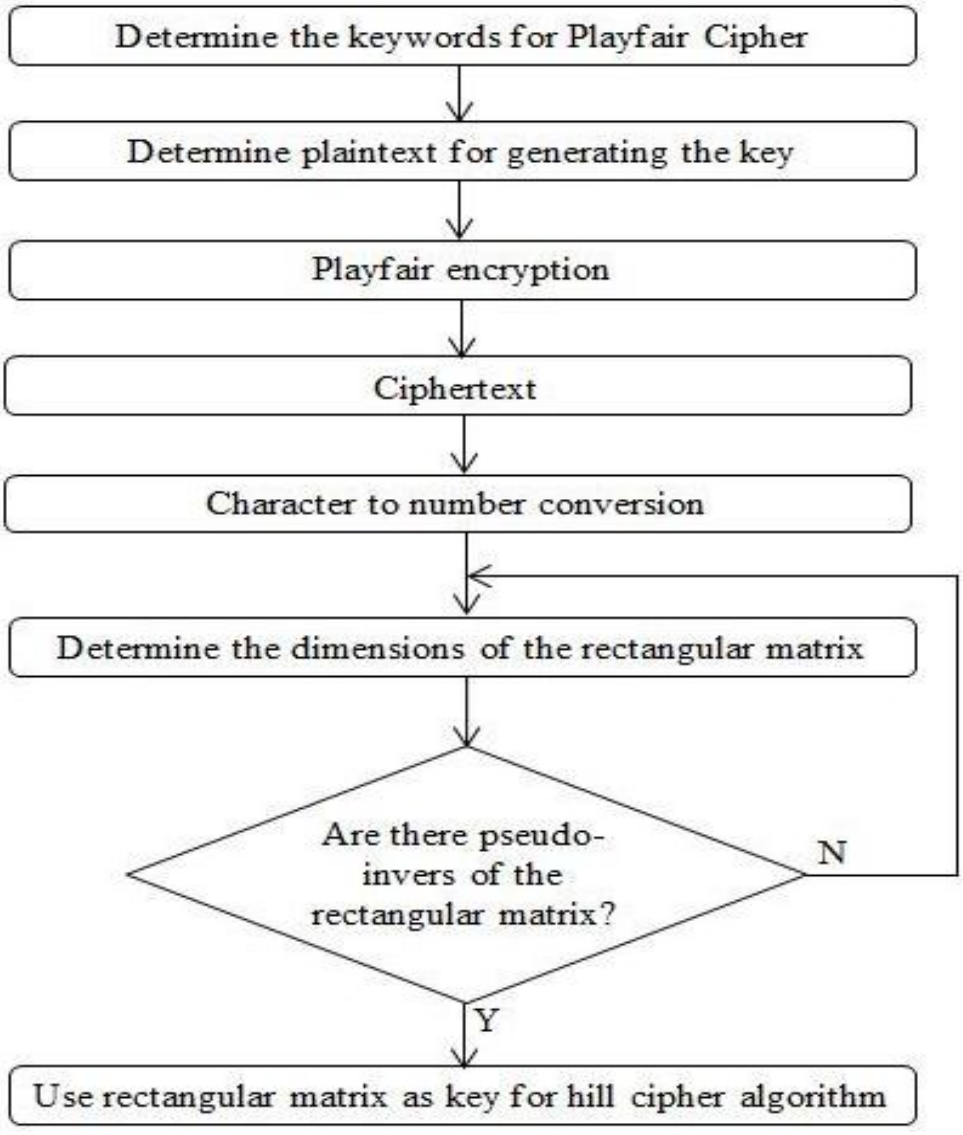

Figure 1. Generation of rectangular matrix key for hill cipher

The encryption process is done by checking the shape of a rectangular matrix key. if the rectangular matrix key has a full column rank, the encryption process uses equations C = KP mod 95. But if the rectangular matrix key has full row rank, then the encryption process uses equations C= PK mod 95 as illustrated in figure 2

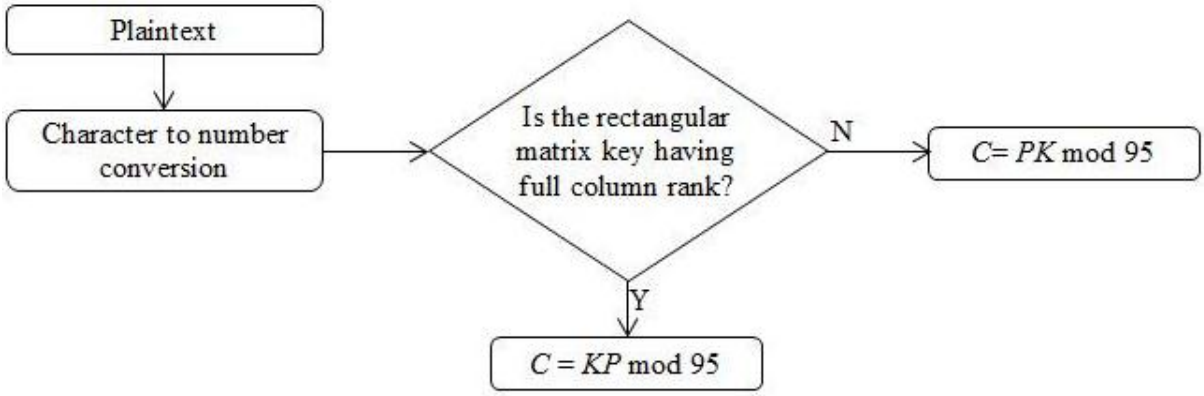

Figure 2. Hill cipher encryption and decryption method

3. Result and Discussion

In the hill cipher algorithm, the process starts with key matrix initialization. Usually key matrix are generated randomly. But in this study the matrix key will be built from the encryption using the Playfair Cipher algorithm. The process starts with creating keywords, for example "rainbow". Then arrange keywords in the matrix by completing letters of the alphabet that are not yet listed in the keywords.

$$\begin{bmatrix} R & A & I & N & B \\ O & W & C & D & E \\ F & G & H & K & L \\ M & P & Q & S & T \\ U & V & X & Y & Z \end{bmatrix} \rightarrow \begin{bmatrix} R & A & I & N & B & R \\ O & W & C & D & E & O \\ F & G & H & K & L & F \\ M & P & Q & S & T & M \\ U & V & X & Y & Z & U \\ R & A & I & N & B & \end{bmatrix}$$

Determine the plaintext for generating the key, example "research report". By using the playfair cipher algorithm it is obtained ciphertext "BO TD IA HQ BO MW BM" and it's corresponding numeral alphabets value is 2 15 20 4 9 1 8 17 2 15 13 23 2 13 with length is 14. Suppose the key rectangular matrix K_{2x7}

$$K = \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \text{ with pseudo invers } K^1 = \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix}$$

If the rectangular matrix chosen does not have a pseudo-inverse matrix, we should get another dimension of rectangular matrix till we get the rectangular matrix that have a pseudo-invers. The rectangular matrix with pseudo-invers can be used as rectangular matrix key for hill cipher algorithm if eligible as:

(i) $KK^{-1}K = K$
(ii) $K^{-1}KK^{-1} = K^{-1}$
(iii) $(KK^{-1})^H = KK^{-1}$
(iv) $(K^{-1}K)^H = K^{-1}K$

The rectangular matrix K is eligible as key matrix for hill cipher algorithm. For example, the plaintext P to be encrypted is "secret message". In this research, hill cipher algorithm using modulus operations 95, let the plaintext conversion into numeric form as on table 1.

Table 1. Character to number correspondence

Char	Value	Char	Value	Char	Value	Char	Value	Char	Value
A	0	T	19	m	38	5	57	}	76
B	1	U	20	n	39	6	58	\	77
C	2	V	21	o	40	7	59	|	78
D	3	W	22	p	41	8	60	‘	79
E	4	X	23	q	42	9	61	∼	80
F	5	Y	24	r	43	spasi	62	!	81
G	6	Z	25	s	44	,	63	@	82
H	7	a	26	t	45	<	64	#	83
I	8	b	27	u	46	.	65	$	84
J	9	c	28	v	47	>	66	%	85
K	10	d	29	w	48	/	67	∧	86
L	11	e	30	x	49	?	68	&	87
M	12	f	31	y	50	;	69	*	88
N	13	g	32	z	51	:	70	(	89
O	14	h	33	0	52	’	71	)	90
P	15	i	34	1	53	”	72	-	91
Q	16	j	35	2	54	[	73	_	92
R	17	k	36	3	55	{	74	=	93
S	18	l	37	4	56	]	75	+	94

The plaintext P "Secret message" corresponding with "18 30 28 43 30 45 62 38 30 44 44 26 32 30" Because the rectangular matrix key is full row ranks, To encrypt P using C = PK mod 95, and partition P into several matrix with each element 2 like the number of rectangular matrix key rows.

$$C_1 = \begin{bmatrix}18 & 30\end{bmatrix} = \begin{bmatrix}2 & 15 & 20 & 4 & 9 & 1 & 8\\ 17 & 2 & 15 & 13 & 23 & 2 & 13\end{bmatrix} mod(95) = \begin{bmatrix}71 & 45 & 50 & 82 & 92 & 78 & 59\end{bmatrix}$$

$$\vdots$$

$$C_7 = \begin{bmatrix}32 & 30\end{bmatrix} = \begin{bmatrix}2 & 15 & 20 & 4 & 9 & 1 & 8\\ 17 & 2 & 15 & 13 & 23 & 2 & 13\end{bmatrix} mod(95) = \begin{bmatrix}4 & 65 & 45 & 43 & 28 & 92 & 76\end{bmatrix}$$

The result as ciphertext C = 71 45 50 82 92 78 59 27 31 65 6 6 19 23 65 65 40 40 70 25 65 10 56 5 77 7 43 40 48 63 25 27 4723 52 55 47 35 39 44 1 25 4 65 45 43 28 92 76 and it's corresponding with 'ty@_|7bf.GGTX..oo:Z.K4F\Hrow,ZbEHX03vjnsBZE.trc_}

To decrypt C using P = C K-1 mod 95

$$P_1 = \begin{bmatrix}71 & 45 & 50 & 82 & 92 & 78 & 59\end{bmatrix} \begin{bmatrix}35 & 38\\ 29 & 4\\ 90 & 25\\ 93 & 4\\ 8 & 69\\ 2 & 51\\ 60 & 72\end{bmatrix} mod(95) = \begin{bmatrix}18 & 30\end{bmatrix}$$

$$\vdots$$

$$P_7 = \begin{bmatrix}4 & 65 & 45 & 43 & 28 & 92 & 76\end{bmatrix} \begin{bmatrix}35 & 38\\ 29 & 4\\ 90 & 25\\ 93 & 4\\ 8 & 69\\ 2 & 51\\ 60 & 72\end{bmatrix} mod(95) = \begin{bmatrix}32 & 30\end{bmatrix}$$

The result as plaintext P = 18 30 ... 32, 30 and it's corresponding with "Secret message"

4. Conclusions

Playfair cipher algorithm can simplify the making of rectangular matrix keys. This will make it easier to remember and distribute the keys used in the hill cipher algorithm. The use of a rectangular matrix key also disguises the message because the ciphertext produced is longer and more random. This will complicate the cryptanalyst in finding the ciphertext linear equation with its matrix key.

References

[1] Alawiyah T, 2017 Pemanfaatan Kunjungan Pohon Biner Pada Kriptografi Hill Cipher Kunci Matriks Persegi Panjang 2, 1 p. 77–82.
[2] Dawahdeh Z E Yaakob S N and Razif bin Othman R, 2018 A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher J. King Saud Univ. - Comput. Inf. Sci. 30, 3 p. 349–355.
[3] Reddy K A Vishnuvardhan B Madhuviswanatham and Krishna A V N, 2012 A Modified Hill Cipher Based on Circulant Matrices Procedia Technol. 4 p. 114–118.
[4] Shostack A, 2014 Threat Modeling: Designing for Security John Willey & Sons, Inc.
[5] Khalaf A A M El-Karim M S A and Hamed H F A, 2016 A triple hill cipher algorithm proposed to increase the security of encrypted binary dataand its implementation using FPGA in International Conference on Advanced Communication Technology, ICACT 2016-March p. 752–759.
[6] Mahendran R and Mani K, 2017 Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher in Proceedings - 2nd World Congress on Computing and Communication Technologies, WCCCT 2017 p. 51–54.
[7] Hidayat A and Alawiyah T, Apr. 2013 Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang J. Mat. Integr. 9, 1 p. 39.