Indonesian Journal of Mathematics Education
Vol. 2, No. 1, April 2019, pp: 9~13
p-ISSN: 2654-3907, e-ISSN: 2654-346X
e-mail: ijome@untidar.ac.id, website: jurnal.untidar.ac.id/index.php/ijome

Hill Cipher Cryptosystem over Complex Numbers

Maxrizal[1a)]
[1]STMIK Atma Luhur, Jl. Jend. Sudirman Selindung, Pangkalpinang, Indonesia
e-mail: [a)]maxrizal@atmaluhur.ac.id

Received: 25 February 2019 *Revised: 8 April 2019* *Accepted: 24 April 2019*

Abstract

The Hill Cipher cryptosystem is a symmetry key cryptosystem. This cryptosystem uses the concept of integer over modulo p. This cryptosystem uses a matrix K as a secret key. We must choose the key matrix K which has an inverse in modulo p. This secret key matrix will be used by the sender and recipient of the message to encrypt and descript the message. For this reason, this paper will discuss the generalization of Hill Cipher using matrices over complex numbers. Calculation of determinants and inverses of the matrix K will adopt a system of determinant and inverse calculations on Hill Cipher. The results show that the proposed cryptosystem scrambles the plaintext.

Keywords: complex numbers, cryptosystem over complex numbers, Hill Cipher cryptosystem

INTRODUCTION

The Hill Cipher cryptosystem is a cryptosystem that uses symmetry keys (Anton & Rorres, 2004). In this cryptosystem, the recipient and sender of the message have the same key and are confidential. This system encrypts message $C = KP \bmod p$ and description $P = K^{-1}C \bmod p$ (Khalaf et al., 2016). In its development, the system is modified in the circulant matrix, involutory matrix and combination of the robust cryptosystem (Acharya et al., 2010). The Hill Cipher cryptosystem was also developed in image encoding (L, 2017), plaintext randomization (Krishna & Madhuravani, 2012), and looping of the Hill Ciphers cryptosystem (Dummit & Foote, 2004).

Suppose there is a message $P = 1-1-4-2-3-5-2-1$. We form the plaintext matrix $P = \begin{bmatrix} 1 & 1 & 4 & 2 \\ 3 & 5 & 2 & 1 \end{bmatrix}$ and select any key matrix $K = \begin{bmatrix} 2 & 12 \\ 3 & 1 \end{bmatrix}$. We use $p = 26$ $(A = 1, B = 2, \ldots, Z = 26)$ to symbolize letters.

Next, we encrypt $C = KP \bmod p = \begin{bmatrix} 12 & 10 & 6 & 16 \\ 6 & 8 & 14 & 7 \end{bmatrix} \bmod 26$. We get ciphertext $12-10-6-16-6-8-14-7$.

Furthermore, if the message $P = 1-1-4-2-3-5-2-1$ we modify over the complex number, we get $P^* = \begin{bmatrix} 1+i & 4+2i \\ 3+5i & 2+i \end{bmatrix}$. If we choose any $K^* = \begin{bmatrix} 2+i & 12+2i \\ 3+2i & 1+4i \end{bmatrix}$ then we do encryption $C = K^*P^* \bmod 26 = \begin{bmatrix} 1+17i & 2+24i \\ 10+22i & 6+23i \end{bmatrix} \bmod 26.$ We get ciphertext $1-17-1-24-10-22-6-23$.

Based on the facts above, we can modify the Hill Cipher cryptosystem over the complex numbers. For this reason, this paper will develop a Hill Cipher cryptosystem that is extended to complex numbers over modules *n*.

METHOD

This research is a literature study. There are references used as a comparison for modifications that have been made to the Hill Cipher cryptosystem. Acharya et al. (2010) discussed the privacy protection of biometric traits using modified Hill Cipher with involuntary key and robust cryptosystem, whereas Krishna & Madhuravani (2012) discussed a modified Hill Cipher using randomized approach and L (2017) studied a modified Hill Cipher based image encryption technique. In their paper, Khalaf et al. (2016) studied a triple Hill Cipher algorithm proposed to increased the security of encrypted binary data, whereas Reddy et al. (2012) discussed a modified Hill Cipher based on circulant matrices, and a modified Hill Cipher for large block of plaintext with interlacing and iteration was studied by Sastry Ravi (2008). Furthermore, the basic properties of the matrix for complex numbers were studied by Lang (1993).

RESULTS AND DISCUSSION

Properties of the Complex Numbers

Complex numbers are a combination of Real numbers and Imaginary numbers. If $z = 2 + 3i$ then $\mathrm{Re}(z) = 2$ and $\mathrm{Im}(z) = 3$. If there is an $z_1, z_2 \in \mathbb{C}$ then apply

$$\begin{aligned} z_1 + z_2 &= (a + bi) + (c + di) \\ &= (a + c) + (b + d)i \\ z_1.z_2 &= (a + bi)(c + di) \\ &= (ac - bd) + (ad + bc)i \end{aligned}$$

Note that $i^2 = -1$ applies. In this paper, a matrix of complex numbers is defined as a matrix whose entries are complex numbers. Suppose is formed a matrix $A = \begin{bmatrix} 2+4i & 3+i \\ 7+2i & 5+4i \end{bmatrix}$.

Hill Cipher Cryptosystem over Complex Numbers

The proposed Hill Cipher cryptosystem uses the same algorithm as the Hill Cipher cryptosystem. The proposed cryptosystem uses a matrix with entries in the form of complex numbers. Suppose there is a plaintext $P = 11 - 14 - 2 - 3 - 5 - 7 - 23 - 12$ and selected a matrix key K of size $n \times n$. If done on the Crypto Hill Cipher system, the plaintext block becomes $P = \begin{bmatrix} 11 & 14 & 2 & 3 \\ 5 & 7 & 23 & 12 \end{bmatrix}$. If we do the proposed cryptosystem then the plaintext form becomes $P^* = \begin{bmatrix} 11+14i & 2+3i \\ 5+7i & 23+12i \end{bmatrix}$. In fact, the size of the plaintext matrix between the two cryptosystems is different. Next, we review plaintext

$$\begin{aligned} P^* &= \begin{bmatrix} 11+14i & 2+3i \\ 5+7i & 23+12i \end{bmatrix} \\ &= \begin{bmatrix} 11 & 2 \\ 5 & 23 \end{bmatrix} + \begin{bmatrix} 14 & 3 \\ 7 & 12 \end{bmatrix} i \end{aligned}$$

This means $P^* = M + Ni$, with M, N being any matrix.

In general, if there is a matrix of keys K and plaintext P, then the Hill Cipher cryptosystem is encrypted $C = KP \bmod p$. Whereas the cryptosystem proposed applies

$$\begin{aligned} C &= KP \bmod p \\ &= (M + Ni)(X + Yi) \bmod p \\ &= (MX - NY) + (MY + NX)i \end{aligned}$$

Note that the mathematical equation in the proposed cryptosystem more randomize ciphertext.

Determinants of Key Matrices in Hill Cipher Cryptosystems over Complex Numbers

In the description of the Hill Cipher cryptosystem, we need a matrix K that has an inverse of modulo n. The main characteristic of a matrix K having an inverse is that the determinant K is not zero and has an inverse in modulo n. Suppose $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is then $\det(A) = ad - bc$. Note that $A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ applies.

In the description of the proposed cryptosystem, we use the same concept in calculating determinants and inverses. Suppose a matrix $K=\begin{bmatrix}3+2i & 5+7i\\ 7+4i & 3+2i\end{bmatrix}$. Next, we calculate the value of

$$\begin{aligned}\det(A) &= (-2-57i) \bmod 26\\ &= (24+21i) \bmod 26\end{aligned}.$$

We will look for a complex number $z=c+di$ so that it applies $(24+21i)(c+di)=1 \pmod{26}$. Note that mathematically $(24+21i)(8+19i) \bmod 26 = -207+624i = 1+0i = 1$. So, we get $\left[\det(A)\right]^{-1} = (8+19i) \bmod 26$.

In general, suppose that $z_1=a+bi$, $z_2=c+di$ and we form $z_1 z_2 = 1$, then apply

$$\begin{aligned}z_1 z_2 &= 1+0i\\ (a+bi)(c+di) &= 1+0i\\ (ac-bd)+(ad+bc)i &= 1+0i\end{aligned}$$

If $b=d=0$ then apply $ac=1$. If $a=3$ then we get a multiplication inverse of modulo 26, namely $c=9$. Note that $ac = 27 \pmod{26} = 1 \pmod{26}$ applies. The following is the multiplication inverse table for modulo 26.

Table 1. The Inverse Multiplication Element Table in Modulo 26

a	1	3	5	7	9	11
a^{-1}	1	9	21	15	3	19
a	15	17	19	21	23	25
a^{-1}	7	23	11	5	17	25

We look again at equation $(ac-bd)+(ad+bc)i=1+0i$. In general, we get $ac-bd=1 \pmod{26}$ and $ad+bc=0 \pmod{26}$. We do the second equation and get $d=\frac{-bc}{a}$. Next, we substitute for the first equation

$$\begin{aligned}ac-b\left(\frac{-bc}{a}\right) &= 1\\ ac+\frac{b^2c}{a} &= 1\\ a^2c+b^2c &= a\\ c &= \frac{a}{a^2+b^2}\end{aligned}$$

Thus we get $c=a\left(a^2+b^2\right)^{-1} \pmod{26}$. Next, we define c in the second equation, $c=\frac{-ad}{b}$. Next, we substitute back to the first equation

$$\begin{aligned}a\left(\frac{-ad}{b}\right)-bd &= 1\\ \frac{-a^2d}{b}-bd &= 1\\ a^2d+b^2d &= -b\\ d &= \frac{-b}{a^2+b^2}\end{aligned}$$

Thus we get $d=-b\left(a^2+b^2\right)^{-1} \pmod{26}$. Note that, $\left(a^2+b^2\right)$ must have an inverse multiplication element in modulo 26.

Suppose there is $z=1+2i$ then $a^2+b^2=5 \pmod{26}$. Based on the multiplication inverse element table in modulo 26, it applies $\left(a^2+b^2\right)^{-1}=21 \pmod{26}$. Thus, we get

$$\begin{aligned}c &= a\left(a^2+b^2\right)^{-1} \pmod{26}\\ &= 21 \pmod{26}\\ d &= -b\left(a^2+b^2\right)^{-1} \pmod{26}\\ &= 10 \pmod{26}\end{aligned}$$

So, we get $(1+2i)^{-1}=(21+10i) \pmod{26}$.

Plaintext Arrangement Rules

If a key matrix is size 2×2, the plaintext will be of size $2\times p$, with $p=ceiling\left(\frac{c}{4}\right)=\left\lceil\frac{c}{4}\right\rceil$ and c being the number

of alphabet messages. Suppose we select the key matrix 2×2 and $c=9$ then $p=\left\lceil \frac{9}{4} \right\rceil =3$. So, we get the size of plaintext 2×3. Suppose there is a plaintext $12-3-5-4-2-11-21-1-8$. Thus, we get $P=\begin{bmatrix} 12+3i & 5+4i & 2+11i \\ 21+i & 8+0i & 0+0i \end{bmatrix}$. Note that there are 3 zero elements (dummy elements) to complete the matrix *P*. In general, if a matrix $n\times n$ is chosen then $p=\left\lceil \frac{c}{2n} \right\rceil$.

Example of a Hill Cipher Cryptosystem over Complex Numbers

Bob will send a message to Alice. Bob and Alice agreed to use the key $K=\begin{bmatrix} 3+2i & 5+i \\ 7+4i & 3+2i \end{bmatrix}$. Before that, Bob must investigate whether *K* has a multiplication inverse in modulo 26. If $\left[\det(K)\right]^{-1}$ exists, the matrix *K* has an inverse. Bob counts

$$\begin{aligned} \det(K) &= -26-15i \pmod{26} \\ &= 11i \pmod{26} \end{aligned}$$

and he gets $a=0$ and $b=11$. Next, Bob calculates $\left(a^2+b^2\right)=121=17\pmod{26}$. Based on the inverse table of the multiplication element in modulo 26, Bob gets $\left(a^2+b^2\right)^{-1}=17^{-1}=23\pmod{26}$. Then, he counts

$$\begin{aligned} c &= a\left(a^2+b^2\right)^{-1}\pmod{26} \\ &= 0\pmod{26} \\ d &= -b\left(a^2+b^2\right)^{-1}\pmod{26} \\ &= 7\pmod{26} \end{aligned}$$

So, Bob gets $\left[\det(K)\right]^{-1}=0+7i=7i$.

Suppose Bob will send a message "LETS GO FISHING NOW". Note the conversion table used below.

Table 2. Letter Conversion Table

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

Based on the conversion table above obtained $P=12-5-20-19-7-15-6-9-19-8-9-14-7-14-15-23$. Next, he changes the plaintext *P* to

$$P=\begin{bmatrix} 12+5i & 20+19i & 7+15i & 6+9i \\ 19+8i & 9+14i & 7+14i & 15+23i \end{bmatrix}.$$

Encryption

Bob encrypts and calculates

$$\begin{aligned} C &= KP \pmod{p} \\ &= \begin{bmatrix} 3+2i & 5+i \\ 7+4i & 3+2i \end{bmatrix} P \\ &= \begin{bmatrix} 9+20i & 1+20i & 12+6i & 13i \\ 1+15i & 11+13i & 8+7i & 5+4i \end{bmatrix} \bmod 26 \end{aligned}$$

Bob obtained the ciphertext $C=9-20-1-20-12-6-0-13-1-15-11-13-8-7-5-4$. Bob got the message "ITATLFZMAOKMHGED". Next, the ciphertext is sent to Alice.

Description

Alice receives a ciphertext from Bob. Alice counts $\left[\det(K)\right]^{-1}=0+7i=7i$. Next, she calculates

$$\begin{aligned} K^{-1} &= (ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \\ &= 7i\begin{bmatrix} 3+2i & -(5+i) \\ -(7+4i) & 3+2i \end{bmatrix} \\ &= \begin{bmatrix} 12+21i & 7+17i \\ 2+3i & 12+21i \end{bmatrix} \pmod{26} \end{aligned}$$

She made a description

$$P = K^{-1}C \pmod{p}$$
$$= \begin{bmatrix} 12+5i & 20+19i & 7+15i & 6+9i \\ 19+8i & 9+14i & 7+14i & 15+23i \end{bmatrix} \pmod{26}$$

Alice gets a message $P = 12-5-20-19-7-15-6-9-19-8-9-14-7-14-15-23$. Based on the conversion table, he gets "LETS GO FISHING NOW".

CONCLUSION

Based on the results and discussion above, we can conclude that the Hill Cipher cryptosystem can be generalized to matrices over complex numbers. The proposed cryptosystem can also produce more random ciphertexts. Furthermore, the concept of a matrix of complex numbers can be considered for various cryptosystems with key symmetry and asymmetry.

REFERENCES

Acharya, B., Sharma, M. D., Tiwari, S., & Minz, V. K. (2010). Privacy Protection of Biometric Traits Using Modified Hill Cipher with Involutory Key and Robust Cryptosystem. *Procedia Computer Science*, *2*, 242–247. https://doi.org/10.1016/j.procs.2010.11.031

Anton, H., & Rorres, C. (2004). *Elementary Linear Algebra: Applications Version*. Wiley eGrade.

Dummit, D. S., & Foote, R. M. (2004). *Abstract Algebra* (3rd ed.). John Wiley & Sons Inc.

Khalaf, A. A. M., El-Karim, M. S. A., & Hamed, H. F. A. (2016). A Triple Hill Cipher Algorithm Proposed to Increase The Security of Encrypted Binary Data and its Implementation Using FPGA. *ICACT Transactions on Advanced Communications Technology (TACT)*, *5*(1), 752–759. https://doi.org/10.1109/ICACT.2016.7423615

Krishna, A. V. ., & Madhuravani, K. (2012). A Modified Hill Cipher Using Randomized Approach. *International Journal of Computer Network and Information Security*, *5*, 56–62. https://doi.org/10.5815/ijcnis.2012.05.07

L, G. (2017). Modified Hill Cipher Based Image Encryption Technique. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, *5*(4), 342–345. https://doi.org/10.22214/ijraset.2017.4063

Lang, S. (1993). *Linear Algebra*. New York: Springer.

Reddy, K. A., Vishnuvardhan, B., Madhuviswanatham, & Krishna, A. V. N. (2012). A Modified Hill Cipher Based on Circulant Matrices. *Procedia Technology*, *4*, 114–118. https://doi.org/10.1016/j.protcy.2012.05.016

Sastry, V. U. K., & Ravi, S. N. (2008). Modified Hill Cipher for a Large Block of Plaintext with Interlacing and Iteration. *Journal of Computer Science*, *4*(1), 15–20. https://doi.org/10.3844/jcssp.2008.15.20