Titian Ilmu: Jurnal Ilmiah Multi Sciences, Vol. 15 No. 2, Halaman: 119 – 124, 2023
https://doi.org/10.30599/jti.v15i2.2850

Application of Extended Euclid Algorithm on Hill Cipher Cryptography Modulo 95

Annisa Nur Azizah[1]*, Nikken Prima Puspita[2], Nurdin Bachtiar[3] and Eriska Meiyana[4]
[1,4] Universitas Nurul Huda
[2,3] Universitas Diponegoro
* E-mail: annisazizah@unuha.ac.id

Abstract

Hill Cipher Cryptography is the art of hiding a message using an invertible matrix as the key. Let A be a 2×2 invertible matrix of the real number. Encryption performed by converting each character on the original message into an ASCII code. The result of the conversion is multiplied by matrix A using matrix multiplication operation modulo 95 which result added with 32. The calculation result in the form of numbers is re-converted into characters according to the ASCII code. It is described in parallel, while the ciphertext matrix is operated using matrix A^(-1). Since matrix A is an invertible matrix and not supposed to have 1/-1 determinant, the matrix result is possibly a non-integer real number. Therefore, the extended Euclid algorithm is needed to finish the description process for finding out the modulo 95 number of a non-integer real number.

Keyword: Extended Euclid, Hill Cipher, Modulo 95, Cryptography.

INTRODUCTION

The development of technology, information and communication in the current era is very fast. But the development of technology often causes information messages to be conveyed to other parties to be not secure because of unauthorized eavesdropping on the message. One way to maintain the confidentiality of the message is to use cryptography. Cryptography is the art of storing or keeping messages from unauthorized recipients. In this case the original message from the sender is called plaintext, while the hidden message is called a ciphertext.

In a paper entitled "Kriptografi Hill Cipher dengan Menggunakan Operasi Matriks" by (Puspita & Nurdin, 2010), they discussed the application of linear algebra specifically cryptographic matrix operations. The idea is to select a $n \times n$ matrix *A* which has a determinant of 1/−1, each letter in the plaintext is marked with a number based on ASCII, then plaintext is partitioned into a matrix $n \times 1$ column. Each column matrix is multiplied by the matrix *A.*The multiplication results obtained are converted back into alphabet using modulo arithmetic rules. This result is the ciphertext. To be able to read the original message from the sender, the recipient must convert the ciphertext to plaintext with the same algorithm but the matrix used is A^{-1} (Puspita & Nurdin, 2010). While in this article, the author will develop the paper by not providing conditions for taking the matrix A, it does not have to have a determinant of 1 / −1 and the element of A is any real number. Because the results obtained will be converted into integers modulo 95, then the resulting value must be an integer. But because the matrix element is a real number, it will require an algorithm which will convert non integer numbers into integers, the algorithm in question is Extended Euclid Algorithm.

LITERATURE REVIEW

Cryptography

Cryptography comes from the Greek language *crypto* and *graphia*. *Crypto* means to hide, and graphia has the meaning of writing. So a cryptography is a mathematical study related to aspects related to information security such as how to hide data contents, prevent data being changed without being detected, or prevent data from being used without sufficient authority (Alfred J. , Paul C, & Scott A,

1996). In cryptography, messages / information that can be read are called plaintext. While the message/information that has been encoded is called ciphertext. Then the encoding process that changes plainteks into a ciphertext is called encryption. Whereas the reverse process for converting the ciphertext into a plaintext is called decryption. In the process of encryption and decryption requires a special mechanism and key that is only known by the sender and recipient of the message.

Cryptographic algorithm or cipher is mathematical functions that are used to do a prosess encryption and description (Schneier, 1996). Cryptographic algorithms are divided into two parts, namely symmetrical algorithms and asymmetric algorithms. *Symmetrical* algorithms are algorithms that use the same encryption key as the description key. In this case the sender and receiver must agree on the key that will be used in the communication process. Leaking the key to an unauthorized person causes a loss of confidentiality. So the security of this algorithm depends on the key. This algorithm is also called secret key algorithm or one key algorithm. *An asymmetric algorithm* , also known as a public key algorithm, uses two keys, the public key and the secret key. Public keys are used to encrypt messages while secret keys are used to decrypt messages.

The Hill cipher was created by Lester S. Hill in 1929. This cryptographic technique was devised to create a cipher (code) that cannot be cracked using frequency analysis techniques (Forouzan, 2008). The Hill cipher employs matrix multiplication as the basis for both encryption and decryption processes. The Hill cipher is a polyalphabetic cipher and can be categorized as a block cipher because the text to be processed is divided into blocks of a specific size. Each character within one block will influence other characters in the encryption and decryption processes, ensuring that the same character does not map to the same character.

The fundamental technique of the Hill Cipher involves modulo arithmetic with matrices. In its application, the Hill Cipher uses matrix multiplication and inversion techniques with matrices. The matrices used in the Hill Cipher are invertible matrices, which are square matrices of size $n \times n$ with a determinant $\neq 0$, ensuring they have an inverse.

Euclid Extended Algorithm

One of the uses of the Euclidean Extended algorithm or what is often referred to as the algorithm *extended Euclid* is to find the inverse modulo occurs if $a \in \mathbb{Z}_n$ so $\gcd(a, n) = 1$. In this case the modulo inverse will be used in the calculation of matrix multiplication. The following are given the steps of the Euclid extension algorithm and the presentation of algorithms in the form of tables as follows (Singh & Singh, 2015).

Table 1. Euclid extension algorithm

$\boldsymbol{Q}$	$\boldsymbol{R_1}$	$\boldsymbol{R_2}$	$\boldsymbol{R}$	$\boldsymbol{T_1}$	$\boldsymbol{T_2}$	$\boldsymbol{T}$
..	..	..	..	..	..	..

- *Q* = Quotient for *R*1 divided by *R*2;
- *R*1 = Modulus value initially, followed by left shift of previous value of *R*2 in later cases.
- *R*2 = Denominator value initially, followed by left shift of value from previous *R* in later cases.
- *R* = Remainder of *R*1 divided by *R*2.
- *T* 1 = 0 initially, followed by left shift of previous value from *T* 2.
- *T* 2 = 1 initially, followed by right shift of previous value from *T* .
- *T* = *T* 1 − *Q* ∗ *T* 2.
- Continue till *R* = 0, and inverse modulo is given by the value at *T* 2.

Here are the steps of the Euclidean Extended algorithm to find the inverse modulo. Steps to find inverse $\boldsymbol{b \bmod a}$:

1. Let $a = R_1$ and $n = R_2$
2. Let $T_1 = 0$, and $T_2 = 1$

3. Count Q, it is quotient R_1/R_2
4. Count $R = R_1 - Q \cdot R_2$ or remainder R_1/R_2
5. Count $T = T_1 - Q \cdot T_2$
6. Next, value of R_1 get from value of R_2 in previous and value of R_2 get from a previous value R
7. Value of T_1 get from a previous value T_2 and value T_2 get from a previous value T.
8. Next count Q, R, T like step in previous. If $R > 0$ so repeat step previous.
9. If $R = 0$ so the step is stop and choose T_2 as a invers

RESULT AND DISCUSSION

Formulation of Hill Cipher Cryptography Algorithm with Matrix

The cryptographic concept which is the application of elementary linear algebra especially the matrix is better known as Hill Cipher. In this paper the author assumes that the reader already understands operations on matrices such as matrix multiplication, looking for matrix determinants and matrix inverses. Before entering into the Hill Cipher encryption algorithm and description, the author needs to inform that each character in the message must first be converted into numbers that conform to the *American Standard Code for Information Interchange. (ASCII*). In this paper the matrix used for the encryption and decryption process is assumed to be a 2x2 matrix with elements A part of real numbers.

Encryption Algorithm

The steps in the encryption process are as follows:
Input: text to be sent.
Process:

1. Select an invertible matrix A of $2x2$. Each element of the matrix A belongs to element $\mathbb{R}$.
$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathbb{R}$$
2. Convert the text being encripted into the ASCII number. Each 2 characters in sequence on the plaintext should be paired. If the last part leaves 1 character only, it could be paired with any dummies in order to fit up the last pair.
3. Convert each plaintext pair p_1p_2 into a column vector $P_1 = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$. Then form the plaintext matrix using the vectors in each column, so that it produces $P = (P_1P_2P_3 \dots P_n)$
4. Then do the multiplicational operation between matrix A and matrix P.
5. Each matrix element obtained from the previous step is taken as an integer of modulo 95 and the result is added with 32. The non integer results which cannot be in the form of modulo 95 can be obtained using Extendet Euclid Algorithm.
6. Finally, convert the resulted numbers into the corresponding ASCII characters.

Output:
Output is text Cipherteks Pc

Decryption Algorithm

The steps in the decryption process are as follows:
Input: Ciphertext Pc that has been obtained from the encryption
Process :

1. Each letter on the ciphertexts inthe form of ASCII characters is converted into the corresponding numbers, and reduced by 32.
2. Next, do the multiplication operation between A^{-1} and the matrix obtained from the step 1, so that it produces plaintext matrix P.
3. Each element of matrix P obtained from the previous step is taken as an integer of modulo 95. the non integer results which cannot be in the form of modulo 95 can be obtained using Extended Euclied Algorithm.

4. The element which are less than 32 should be added with 95. as for those which are more than 32 does not need so. Then, convert the numbers on matrix P into the corresponding ASCII characters.

Output:
Output of the decryption process is the original text sent by the sender

Simulation of Encryption Algorithm

1. Let matrix $A \in \mathbb{R}$

$$A = \begin{pmatrix} 1/4 & 0 \\ 2 & 1 \end{pmatrix}$$

Determinant of $A = \frac{1}{4} - 0 = \frac{1}{4} \neq 0$

2. Let be plainteks is Unuha 2021

Convert the text being encripted into the ASCII number. Each 2 characters in sequence on the plaintext should be paired. If the last part leaves 1 character only, it could be paired with any dummies in order to fit up the last pair.

$$P_1 = \begin{pmatrix} U \\ n \end{pmatrix} = \begin{pmatrix} 85 \\ 110 \end{pmatrix}; P_2 = \begin{pmatrix} u \\ h \end{pmatrix} = \begin{pmatrix} 117 \\ 104 \end{pmatrix};\ P_3 = \begin{pmatrix} a \\ \end{pmatrix} = \begin{pmatrix} 97 \\ 32 \end{pmatrix}$$
$$P_4 = \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 50 \\ 48 \end{pmatrix}; P_5 = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 50 \\ 49 \end{pmatrix}$$

3. Convert each plaintext pair p_1p_2 into a column vector $P_1 = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$. Then form the plaintext matrix using the vectors in each column, so that it produces $P = (P_1P_2P_3 \ldots P_n)$

$$P = \begin{pmatrix} 85 & 117 & 97 & 50 & 50 \\ 110 & 104 & 32 & 48 & 49 \end{pmatrix}$$

4. Then do the multiplicational operation between matrix A and matrix P.

$$AP = \begin{pmatrix} 1/4 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 85 & 117 & 97 & 50 & 50 \\ 110 & 104 & 32 & 48 & 49 \end{pmatrix}$$
$$= \begin{pmatrix} \frac{85}{4} & \frac{117}{4} & \frac{97}{4} & \frac{50}{4} & \frac{50}{4} \\ 280 & 338 & 226 & 148 & 149 \end{pmatrix} mod\ 95$$

Each matrix element obtained from the previous step is taken as an integer of modulo 95 and the result is added with 32. The non integer results which cannot be in the form of modulo 95 can be obtained using Extendet Euclid Algorithm.

Because there are elements that cannot be directly modulated, the inverse of that element must be finded.

$$\frac{1}{4}\ mod\ 95 = \ 4^{-1}(mod\ 95)$$

Table 2. Calculation of euclid extension algorithm

Q	R_1	R_2	R	T_1	T_2	T
23	95	4	3	0	1	72
1	4	3	1	1	72	24
3	3	1	0	72	24	0

So,

$$\frac{85}{4}\ mod\ 95 = (85)\ 4^{-1}(mod\ 95) = 85 \times 24 = 2040$$

$\frac{117}{4} \; mod\; 95 = (117)\; 4^{-1}(mod\; 95) = 117 \times 24 = 2808$
$\frac{97}{4} \; mod\; 95 = (97)\; 4^{-1}(mod\; 95) = 97 \times 24 = 2328$
$\frac{50}{4} \; mod\; 95 = (50)\; 4^{-1}(mod\; 95) = 50 \times 24 = 1200$

Then the value $A.P$ to be

$$A.P = \begin{pmatrix} 2040 & 2808 & 2328 & 1200 & 1200 \\ 280 & 338 & 226 & 148 & 149 \end{pmatrix} mod\; 95$$

$$= \begin{pmatrix} 45 & 53 & 48 & 60 & 60 \\ 90 & 53 & 36 & 53 & 54 \end{pmatrix} + 32$$

$$= \begin{pmatrix} 77 & 85 & 80 & 92 & 92 \\ 122 & 85 & 68 & 85 & 86 \end{pmatrix}$$

5. Finally, convert the resulted numbers into the corresponding ASCII characters.

$$\begin{pmatrix} 77 & 85 & 80 & 92 & 92 \\ 122 & 85 & 68 & 85 & 86 \end{pmatrix}$$

$MzUUPD\backslash U\backslash V$

Simulation of Decryption Algorithm

Input : $MzUUPD\backslash U\backslash V$

Process :

1. Each letter on the ciphertexts inthe form of ASCII characters is converted into the corresponding numbers, and reduced by 32.

$$Pc = \begin{pmatrix} 77 & 85 & 80 & 92 & 92 \\ 122 & 85 & 68 & 85 & 86 \end{pmatrix} - 32$$

$$= \begin{pmatrix} 45 & 53 & 48 & 60 & 60 \\ 90 & 53 & 36 & 53 & 54 \end{pmatrix}$$

2. Next, do the multiplication operation between A^{-1} and the matrix obtained from the step 1, so that it produces plaintext matrix P.

$$A = \begin{pmatrix} 1/4 & 0 \\ 2 & 1 \end{pmatrix},$$

$$A^{-1} = \frac{1}{1/4}\begin{pmatrix} 1 & 0 \\ -2 & 1/4 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ -8 & 1 \end{pmatrix}$$

$$A^{-1}.Pc = \begin{pmatrix} 4 & 0 \\ -8 & 1 \end{pmatrix}\begin{pmatrix} 45 & 53 & 48 & 60 & 60 \\ 90 & 53 & 36 & 53 & 54 \end{pmatrix}$$

$$= \begin{pmatrix} 192 & 212 & 192 & 240 & 240 \\ -270 & -371 & -348 & -427 & -426 \end{pmatrix} mod\; 95$$

$$= \begin{pmatrix} 85 & 117 & 97 & 50 & 50 \\ 110 & 104 & 32 & 48 & 49 \end{pmatrix}$$

3. The element which are less than 32 should be added with 95. as for those which are more than 32 does not need so. Then, conevert the numbers on matrix P into the corresponding ASCII characters.

$$\begin{pmatrix} 85 & 117 & 97 & 50 & 50 \\ 110 & 104 & 32 & 48 & 49 \end{pmatrix}$$

$$\begin{pmatrix} U & u & a & 2 & 2 \\ n & h & & 0 & 1 \end{pmatrix}$$

Output : Unuha 2021

CONCLUSION

Hill Cipher using matrix operations is one simple example of cryptography. By utilizing ASCII character codes and matrix operations, the encryption and decryption process can be done manually by the sender and recipient of the message. Retrieval of matrix A does not have to be an integer, because there is an euclid expansion algorithm which is used to find inverse modulo or to make non integers an integer. The suggestion from this discussion is the need to be developed again regarding this program / application for the use of hill cipher cryptography.

REFERENCES

Alfred J. , M., Paul C, O., & Scott A, V. (1996). *Handbook of Applied Cryptography.* Boca Raton: CRC Press.

Forouzan, B. A. (2008). *Introduction to Cryptography and Network Security.* New York: McGraw-Hill.

Puspita, N. P., & Nurdin, B. (2010). KRIPTOGRAFI HILL CIPHER DENGAN MENGGUNAKAN OPERASI MATRIKS. *Seminar Nasional Ilmu Komputer Universitas Diponegoro.* Semarang: Universitas Diponegoro.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* New York: John Wiley and Sons.

Singh, L. D., & Singh, K. M. (2015). Implementation of Text Encryption using Elliptic Curve Cryptography. *Procedia Computer Science*, 73-82.