Jurnal Mandiri IT
Vol. 12 No. 3, January (2024), pp. 135-141

ISSN 2301-8984 (Print), 2809-1884 (Online)
Published by Institute of Computer Science

Key analysis of the hill cipher algorithm (Study of literature)

Sujarwo
Politeknik Unggul LP3M, Indonesia

ARTICLE INFO

Article history:

Received Dec 23, 2023
Revised Dec 26, 2023
Accepted Jan 13, 2024

Keywords:

Cipher Text;
Hill Cipher;
Matrix;
Modulo;
Plain Text.

ABSTRACT

The security of the data (message) sent is very important in maintaining the confidentiality of the message. Many algorithms can be used to secure messages. Among them is the Hill Cipher algorithm. The Hill Cipher algorithm is a classic cryptographic algorithm. This algorithm uses a square matrix key. In connection with the Hill Cipher algorithm key, this literature aims to examine the matrix that can be used as a key in the encryption and decryption process in the Hill Cipher algorithm. In this literature, we take a square matrix of order 3x3 and use 36 characters (A-Z, 0-9). To produce cipher text, the method used is to carry out an encryption process based on the Hill Cipher algorithm. The encryption process is carried out by multiplying the key matrix by the plaintext. The decryption process to get the plain text back is done by multiplying the ciphertext by the inverse modulo matrix of the key matrix. The encryption process can always be carried out, but not all decryption processes can be carried out. Because not all matrices can be used as key matrices. The results of this literature show that the key matrix must be a matrix of order mxm. A matrix with determinant value = 0 cannot be used as a key. Likewise, a matrix whose determinant value is not relatively prime with the number of characters to be encrypted or decrypted cannot be used as a key matrix.

Corresponding Author:

Sujarwo,
Informatics Management Study Program,
Politeknik Unggul LP3M,
Jl. Iskandar Muda No. 3 EF, Medan 20153, Indonesia.
Email: sujarwo2268@gmail.com

1. INTRODUCTION

Data security and confidentiality is a very important aspect in information systems today (Hasibuan et al., 2022). Cryptography is a branch of science that studies how to secure and protect the information (data) that is sent. The two main concepts of cryptography are encryption and decryption (Hasan et al., 2020). The aim is to maintain the confidentiality of messages sent so that they are not known by unauthorized and irresponsible people. The message is kept secret by randomizing the values contained in it, resulting in a message that is difficult to understand which results in loss of information from the message (Wasil, 2023).

Messages are information, can be in the form of text, images, sound and video (Sujjada & Erlinda Juniar, 2022). One of the classic cryptographic algorithms is the Hill Cipher algorithm. The general forms of classical algorithms are substitution ciphers and transposition ciphers. Substitution ciphers are carried out by replacing (substituting) a letter in the plaintext with another letter in the ciphertext. Types of substitution in cryptography include Single Alphabet Ciphers, Homophonic Substitution Ciphers, Compound Alphabet Ciphers, and Polygram Substitution Ciphers. Examples of classic cryptographic algorithms with substitution cipher form are Vigenere Cipher, Caesar Cipher, and Hill Cipher (Widia Asiani & Yanti, 2022)(Gusmana et al., 2022). This algorithm was created by Lester S. Hill in 1929 (Fadlilah et al., 2022).

The Hill Cipher algorithm uses a matrix of order mxm (square matrix) as the key (Rasudin et al., 2022). The Hill Cipher method is one of several methods in cryptography. This matrix is an invertible matrix (Hasan et al., 2020). Hill Cipher does not replace each of the same letters in the plaintext with other letters that are the same in the ciphertext because it uses matrix multiplication as a basis for encryption and decryption (Endaryono et al., 2021) (Permata Dewi et al., 2022). Because security depends on the confidentiality of the invertible key matrix (Hasoun et al., 2021). For the data encryption process, it is obtained by multiplying the key matrix by the plaintext. And the decryption process is obtained by multiplying the inverse modulo matrix with the ciphertext (Alawiyah et al., 2020) (Hamdani & Junaidi, 2020).

In connection with the use of the inverse modulo matrix in decrypting ciphertext into plaintext again, several rules are needed for the matrix key. In this literature, matrix analysis is used as a key to the Hill Cipher algorithm. The matrix is a matrix with order mxm, a matrix with a determinant not equal to zero, a matrix with a relatively prime determinant value with the number of characters that can be used as plaintext. With a matrix order of mxm, the number of matrices that can be used as keys will be very large. This is the strength of the Hill Cipher algorithm.

2. RESEARCH METHOD

This research method uses the literature method. Takes data with a certain number of characters and encrypts and decrypts it with the Hill Cipher Algorithm. The key used in the encryption and decryption process uses a 3x3 matrix. Done with different matrix determinant values. While the supporting theory is:

2.1 Modulo

If a and m are integers and m > 0, according to the division rule a divided by m remains r or a mod m = r and can be expressed as a = mq + r, where $0 \leq r < m$ (Rahma, Rahmawati, & Zukrianto, 2020). Example 9 mod 4 = 1, which means that 9 = 4x2 + 1, or can be expressed as $9 \equiv 1 \pmod 4$. Next, find the inverse modulo based on $aa^{-1} \equiv 1 \bmod m$ equivalent to$aa^{-1} = mq + r$ so that $a^{-1} = \frac{mq+1}{a}$

2.2 Matrix

For example $A_{mxm} = [a_{ij}]$, hence the minor of a_{ij}, which is symbolized by M_{ij}, is the determinant of the submatrix A which is obtained by removing all entries in the ith row and all entries in the jth column. While the cofactor of a_{ij} which is symbolized by C_{ij} is $(-1)^{i+j}M_{ij}$. The determinant of the matrix A, can be calculated by multiplying the entries in any row or column by their cofactors and adding up the product where $1 \leq i \leq m$ and $1 \leq j \leq m$ (Rahma, Rahmawati, & Vitho, 2020)

If A and B are square matrices and if matrix B can be found such that AB = BA = I, then A is said to be invertible and B is called the inverse of A and can be written $B = A^{-1}$ (Rahmawati et al., 2020). And the inverse of matrix A can be calculated by

$A^{-1} = \frac{1}{\text{determinant A}} \text{Adjoin (A)} = \frac{1}{\text{determinant A}} C_{ij}^{T}$ (Rahma et al., 2022). Next in finding the inverse of the modulo matrix is

$$A^{-1} = (\text{Inverse modulo from determinant A})\text{Adjoin}(A) = (\text{Inverse modulo dari determinant A})C_{ij}^{T}$$

a. Hill Cipher Encryption Algorithm

The Hill Cipher Encryption Algorithm is used to convert plaintext into ciphertext with the following steps (Hasibuan et al., 2022): (a) Specify the Plaintext (original text) to be encoded. (b) Determine the key matrix and it is an invertible matrix, that is, it has multiplicative inverse K^{-1} so that $K.K^{-1} \equiv I$ (c) Convert plaintext into numerical form according to the predetermined conversion. (d) Counting the number of characters in the plaintext. Next, the number of characters in the plaintext is divided by the order of the specified key matrix. (e) Arrange the numeric plaintext into a matrix (m x 1 if the key order is m x m). (f) Carry out the encryption process by multiplying the key matrix by the plaintext matrix. Next, the result is modulated by n. (g) Convert to letters/text according to the conversion table. Thus, we obtain ciphertext or password characters which are the result of the encryption process.

b. Hill Cipher Decryption Algorithm

The Hill Cipher Decryption Algorithm used to convert cipher text back to plain text is as follows (Fitroti et al., 2021) (a) Correspond alphabetically to numerically. (b) Change the ciphertext to numeric. (c) The key used to decrypt the ciphertext into plaintext is the inverse modulo matrix of the key matrix K (d) Calculating K inverse modulo matrix (K^{-1}) where $K.K^{-1} \equiv I$ (e)Multiply the inverse modulo matrix by the ciphertext that has been transposed in a certain modulo (f) Obtained transposed plaintext $P^T = K^{-1}C^T$ (g)From the 5th point obtained $P = (P^T)^T$

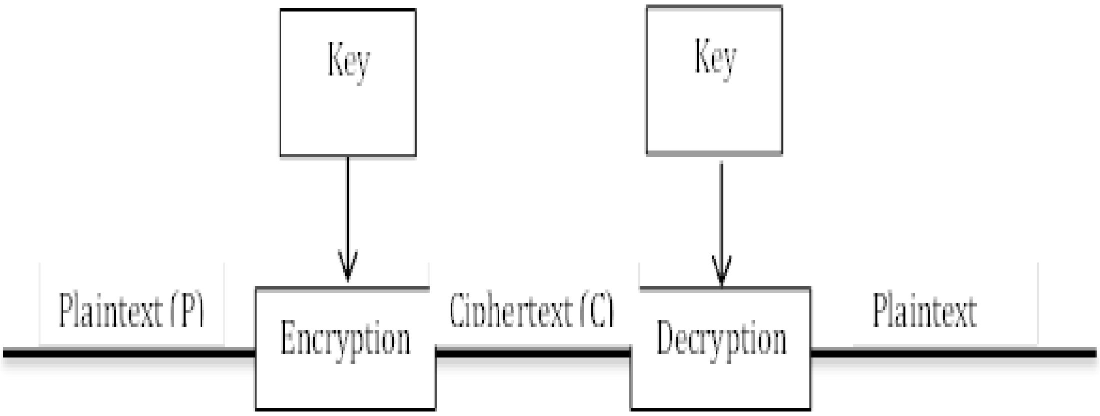

Figure 1. Encryption and descryption

3. RESULTS AND DISCUSSIONS

A message contains the following: TARGET 1268X, where A=0, B=1, ... , Z=25, 0=26, 1=27, ..., 9=35. Encrypted using the Hill Cipher method with a key matrix

$$K = \begin{bmatrix} 2 & 5 & 3 \\ 1 & 2 & 2 \\ 8 & 2 & 7 \end{bmatrix}$$

3.1 Encryption Process

Table 1. Convert plaintext

Plaintext	Number
T	19
A	0
R	17
G	6
E	4
T	19
1	27
2	28
6	32
8	34
X	23
A	0

Because the number of plaintext characters is not enough for a 3x3 matrix key, character A is added. The encryption process is carried out as follows:

For character TAR

$$C = \begin{bmatrix} 2 & 5 & 3 \\ 1 & 2 & 2 \\ 8 & 2 & 7 \end{bmatrix} x \begin{bmatrix} 19 \\ 0 \\ 17 \end{bmatrix} = \begin{bmatrix} 89 \\ 53 \\ 271 \end{bmatrix} \bmod 36 = \begin{bmatrix} 17 \\ 17 \\ 19 \end{bmatrix} = \begin{bmatrix} R \\ R \\ T \end{bmatrix}$$

For character GET

$$C = \begin{bmatrix} 2 & 5 & 3 \\ 1 & 2 & 2 \\ 8 & 2 & 7 \end{bmatrix} x \begin{bmatrix} 6 \\ 4 \\ 19 \end{bmatrix} = \begin{bmatrix} 89 \\ 52 \\ 189 \end{bmatrix} \text{mod } 36 = \begin{bmatrix} 17 \\ 16 \\ 9 \end{bmatrix} = \begin{bmatrix} R \\ Q \\ J \end{bmatrix}$$

For character 126

$$C = \begin{bmatrix} 2 & 5 & 3 \\ 1 & 2 & 2 \\ 8 & 2 & 7 \end{bmatrix} x \begin{bmatrix} 27 \\ 28 \\ 32 \end{bmatrix} = \begin{bmatrix} 290 \\ 147 \\ 496 \end{bmatrix} \text{mod } 36 = \begin{bmatrix} 2 \\ 3 \\ 28 \end{bmatrix} = \begin{bmatrix} C \\ D \\ 2 \end{bmatrix}$$

For character 8XA

$$C = \begin{bmatrix} 2 & 5 & 3 \\ 1 & 2 & 2 \\ 8 & 2 & 7 \end{bmatrix} x \begin{bmatrix} 34 \\ 23 \\ 0 \end{bmatrix} = \begin{bmatrix} 183 \\ 80 \\ 318 \end{bmatrix} \text{mod } 36 = \begin{bmatrix} 3 \\ 8 \\ 30 \end{bmatrix} = \begin{bmatrix} D \\ I \\ 4 \end{bmatrix}$$

The encryption results obtained using the Hill Cipher algorithm are as follows:

Table 2. Encryption results

Plaintext	Ciphertext
T	R
A	R
R	T
G	R
E	Q
T	J
1	C
2	D
6	2
8	D
X	I
A	4

3.2 Decryption Process

The number of possible characters that can be encrypted is 36 (A to Z, 0 to 9). Based on the matrix key K, the determinant value K = 23, the value 36 is relatively prime with 23. It is called relatively prime if there are 2 numbers where the divisors of both numbers are not the same except for factor 1 (YOHANES, 2022). Relatively good at being able to carry out the decryption process. If it is not relatively prime then it is necessary to calculate the number of plaintext characters and the K matrix key.

Inverse The value of the determinant K is K^{-1}, obtained using the formula $K^{-1} = \frac{mq+1}{\text{Det K}}$, for any value of q so that we obtain K^{-1} which is not a fraction, with a value of m=36 (number of characters).

Calculations to find the value of K^{-1} with m=36 then $K^{-1} = \frac{36q+1}{23}$ are obtained as follows.

Table 3. Calculations to determine K^{-1}

q	K^{-1}
1	1.6087
2	3.1739
3	4.7391
4	6.3043
5	7.8696
6	9.4348
7	11.0000
8	12.5652
9	14.1304
10	15.6957
11	17.2609
12	18.8261

Based on the calculation above with q=7, we get K^{-1}=11 (value without decimals)

Matrix cofactors K

$$\text{Cofactors K} = \begin{bmatrix} 10 & 9 & -14 \\ -29 & -10 & 36 \\ 4 & -1 & -1 \end{bmatrix}$$

Adjoint matrix K

$$\text{Adjoint K} = \begin{bmatrix} 10 & -29 & 4 \\ 9 & -10 & -1 \\ -14 & 36 & -1 \end{bmatrix}$$

The inverse of the matrix K modulo 36 is

$$K^{-1} = 11 \begin{bmatrix} 10 & -29 & 4 \\ 9 & -10 & -1 \\ -14 & 36 & -1 \end{bmatrix} \text{mod } 36 = \begin{bmatrix} 2 & 5 & 8 \\ 27 & 34 & 25 \\ 26 & 0 & 25 \end{bmatrix}$$

Decryption of Ciphertext

Table 4. Convert ciphertext

Ciphertext	Number
R	17
R	17
T	19
R	17
Q	16
J	9
C	2
D	3
2	28
D	3
I	8
4	30

For character RRT

$$P1 = \begin{bmatrix} 2 & 5 & 8 \\ 27 & 34 & 25 \\ 26 & 0 & 25 \end{bmatrix} x \begin{bmatrix} 17 \\ 17 \\ 19 \end{bmatrix} = \begin{bmatrix} 271 \\ 1512 \\ 917 \end{bmatrix} \text{mod } 36 = \begin{bmatrix} 19 \\ 0 \\ 17 \end{bmatrix} = \begin{bmatrix} T \\ A \\ R \end{bmatrix}$$

And so on for ciphertext R, Q, J, C, D, 2, D, I, 4, so that the decryption results are obtained

Table 5. Decryption results

Ciphertext	Plaintext
R	T
R	A
T	R
R	G
Q	E
J	T
C	1
D	2
2	6
D	8
I	X
4	A

If the key matrix K is changed to

$$K1 = \begin{bmatrix} 3 & 1 & -2 \\ 4 & 4 & 3 \\ 2 & 1 & 2 \end{bmatrix} \text{ or } K2 = \begin{bmatrix} 1 & 4 & 1 \\ 2 & 5 & 2 \\ 3 & 2 & 3 \end{bmatrix} \text{ or } K3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{bmatrix} \text{ or } K4 = \begin{bmatrix} 2 & 4 \\ -1 & 3 \\ 1 & 2 \end{bmatrix}$$

the determinant value of the matrix K1 = 21. The value 21 is not relatively prime with 36 so we cannot find the inverse of the value 21. The inverse of 21 modulo m is obtained by $K^{-1} = \frac{mq+1}{21}$, which means $K^{-1} = \frac{36q+1}{21}$ no q value causes K^(-1) to produce a whole value (no decimals). Because the value 21 does not have an inverse modulo 36, this matrix cannot be used as a key matrix. Furthermore, the relatively prime numbers with 36 include 5, 7, 11, 13, 17, 19, 25 and so on. If the determinant value of the key matrix is the same as these values, then it can be used as the key matrix for the Hill Cipher algorithm. Likewise for the K2 matrix, the determinant value of K2 = 0. If the determinant value = 0 then the matrix has no inverse. Next are the K3 and K4 matrices, these matrices do not have a determinant value. Thus, the four matrices cannot be used in decryption, so they cannot be used as key matrices for the Hill Cipher algorithm.

4. CONCLUSION

The conclusion from this literature is that the Hill Cipher algorithm uses a matrix as a key in encrypting and decrypting. The matrix used is a matrix of order mxm. For a 3x3 matrix, all plaintext can be encrypted into ciphertext. In decryption, the inverse modulo matrix is used. Not all matrices of order 3x3 can decrypt ciphertext back into plaintext. A matrix that can be used as a key is an invertible matrix, where the determinant of the matrix is not equal to zero and the determinant value of the matrix must be relatively prime with the number of characters that can be used as plaintext.

ACKNOWLEDGEMENTS

I would like to thank all my fellow lecturers and staff at the Politeknik Unggul LP3M, and other researchers who have published their articles in journals, as well as to the Jurnal Mandiri IT team so that this journal can be published.

REFERENCES

Alawiyah, T., Hikmah, A. B., Wiguna, W., Kusmira, M., Sutisna, H., & Simpony, B. K. (2020). Generation Of Rectangular Matrix Key For Hill Cipher Algorithm Using Playfair Cipher. *Journal Of Physics: Conference Series*, *1641*(1). Https://Doi.Org/10.1088/1742-6596/1641/1/012094

Endaryono, E., Dwitiyanti, N., & Setiawan, H. S. (2021). Aplikasi Operasi Matriks Pada Perancangan Simulasi Metode Hill Cipher Menggunakan Microsoft Excel. *String (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(1). Https://Doi.Org/10.30998/String.V6i1.8603

Fadlilah, S. N., Turmudi, T., & Khudzaifah, M. (2022). Penggabungan Algoritma Hill Cipher Dan Elgamal Untuk Mengamankan Pesan Teks. *Jurnal Riset Mahasiswa Matematika*, *1*(5). Https://Doi.Org/10.18860/Jrmm.V1i5.14496

Fitroti, H., Romdhini, M. U., & Switrayni, N. W. (2021). Hill Cipher Algorithm With Generalized Fibonacci Matrix In Message Encoding. *Eigen Mathematics Journal*, *4*(2).

Gusmana, R., Haryansyah, H., & Fitria, F. (2022). Implementasi Algoritma Affine Cipher Dan Caesar Cipher Dalam Mengamankan Data Teks. *Sebatik*, *26*(2). Https://Doi.Org/10.46984/Sebatik.V26i2.2084

Hamdani, D., & Junaidi, J. (2020). Modifikasi Karakter Kode Pada Cipher Hill Menggunakan Kode Ascii. *Eigen Mathematics Journal*. Https://Doi.Org/10.29303/Emj.V3i1.54

Hasan, P., Yunita, S., & Ariyus, D. (2020). Implementasi Hill Cipher Pada Kode Telepon Dan Five Modulus Method Dalam Mengamankan Pesan. *Sisfotenika*, *10*(1). Https://Doi.Org/10.30700/Jst.V10i1.521

Hasibuan, Y. W., Isnarto, I., & Veronica, R. B. (2022). Perancangan Dan Implementasi Aplikasi Kriptografi Algoritma Hill Cipher Dalam Dekripsi Enkripsi Data Keuangan Nasabah Bank Sampoerna Menggunakan Kode Ascii. *Unnes Journal Of Mathematics*, *11*(1). Https://Doi.Org/10.15294/Ujm.V11i1.29356

Hasoun, R. K., Khlebus, S. F., & Tayyeh, H. K. (2021). A New Approach Of Classical Hill Cipher In Public Key Cryptography. *International Journal Of Nonlinear Analysis And Applications*, *12*(2). Https://Doi.Org/10.22075/Ijnaa.2021.5176

Permata Dewi, N., Sembiring, D. J. M., Br. Ginting, R., & Br. Ginting, M. (2022). Pengamanan Data Dengan Kriptografi Hibrida Algoritma Hill Cipher Dan Algoritma Luc Serta Steganografi Chaotic Lsb. *Jurnal Syntax Admiration*, *3*(2). Https://Doi.Org/10.46799/Jsa.V3i2.389

Rahma, A. N., Arisanti, R., Marzuki, C. M. C., & Aryani, F. (2022). Invers Matriks Leslie Bentuk Khusus Ordo N×N (N≥4). *Jurnal Matematika Integratif*, *18*(2). Https://Doi.Org/10.24198/Jmi.V18.N2.40448.127-139

Rahma, A. N., Rahmawati, R., & Vitho, R. H. (2020). Determinan Matriks Segitiga Atas Bentuk Khusus Ordo 3×3 Berpangkat Bilangan Bulat Positif Menggunakan Kofaktor. *Jurnal Sains Matematika Dan Statistika*, *6*(2). Https://Doi.Org/10.24014/Jsms.V6i2.10524

Rahma, A. N., Rahmawati, R., & Zukrianto, Z. (2020). Aplikasi Sistem Modulo 7 Dalam Prediksi Peringatan Hari Besar Nasional Indonesia Tahun 2030. *Map (Mathematics And Applications) Journal*, *2*(2). Https://Doi.Org/10.15548/Map.V2i2.2260

Rahmawati, R., Fitri, N., & Rahma, A. N. (2020). Invers Matriks Rsfplrcircfr (0,B,...,B). *Jurnal Sains Matematika Dan Statistika*, *6*(1). Https://Doi.Org/10.24014/Jsms.V6i1.9260

Rasudin, R., Zulfan, Z., & Rizki, P. (2022). Analisis Perbandingan Keamanan Kriptografi Klasik Pada Algoritma Secure Hill Cipher Berbasis Kode Ascii Dan Monoalphabetic. *Jurnal Teknologi Terapan And Sains ….*

Sujjada, A., & Erlinda Juniar. (2022). Implementasi Algoritma Hill Cipher Untuk Proses Enkripsi Data Menggunakan Media Citra Digital. *Jurnal Restikom : Riset Teknik Informatika Dan Komputer*, *3*(1). Https://Doi.Org/10.52005/Restikom.V3i1.76

Wasil, Moh. (2023). Implementasi Matriks Dalam Kriptografi Hill Cipher Dalam Mengamankan Pesan Rahasia. *Zeta - Math Journal*, *8*(2). Https://Doi.Org/10.31102/Zeta.2023.8.2.71-78

Widia Asiani, R., & Yanti, I. (2022). Penerapan Kriptografi Caesar Cipher Dan Hill Cipher Dalam Pengiriman Pesan Rahasia Sebagai Media Pembelajaran Matematika Realistik Pada Materi Modulo. *Baitul 'Ulum*, *6*(1).

Yohanes, B. (2022). Beban Kognitif Intrinsic Dalam Pembelajaran Materi Eksistensi Bilangan Irrasional. *Edupedia*, *6*(1). Https://Doi.Org/10.24269/Ed.V6i1.1177