# Hill Cipher Order 3 x 3 in Data Encryption and Decryption

**Uc Mariance [1], Andysah Putera Utama Siahaan [1], Siti Rosmiyati [2]**
[1]Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
[2]Degree Student, Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: [1] ucmariance@dosen.pancabudi.ac.id, [1] andiesiahaan@gmail.com, [2] sitirosmiyati2@gmail.com

***Abstract:*** *Cryptography is the art of maintaining the confidentiality and security of data. Several cryptographic algorithms can be applied to maintain data confidentiality. One of them is a popular algorithm to use is Hill Cipher. This algorithm is one of the cryptographic algorithms that use symmetric keys. The Hill Cipher algorithm uses a matrix measuring m x m to do the encryption and decryption process. Hill Cipher is also one of the classic cryptographic algorithms that are very difficult to solve by cryptanalysts if done only by knowing the ciphertext file because this algorithm does not replace each alphabet in the same plaintext with the same alphabet on the ciphertext. This study discusses the Hill Cipher cryptographic method with the order of 3 x 3. This study aims to implement the Hill Cipher cryptographic algorithm in the process of data encryption. The work of this algorithm is high-speed and difficult to solve by irresponsible parties.*

***Keywords:*** *Cryptography, Hill Cipher, Encryption, Decryption.*

## 1. INTRODUCTION:

The development of computer networks in the present time allows us to communicate or send messages through computer networks [1]. One form of communication is using writing. There is much information that can be delivered via digital messages [2]. It is sometimes in sending the information; there is confidential information that must not be known other than the recipient of a legitimate message. Specific methods and techniques can be used to maintain the security of messages that are confidential. One of them is cryptography which functions to disguise messages into encrypted message forms [3]. One of the cryptographic algorithms is the Hill Cipher algorithm, which is the application of cryptographic modulo arithmetic that uses a square matrix as a key to encryption and decryption. Hill Cipher is one of the symmetrical cryptographic algorithms that have the advantage of being resistant to frequency analysis [4]–[6] Hill Cipher algorithm is complicated to solve by cryptanalysts if done only by knowing the ciphertext file [7]. Due to Hill Cipher does not replace each alphabet in the same plaintext with the same alphabet in the ciphertext, it is hard to solve the ciphertext into the plaintext. It uses matrix multiplication when performing encryption and decryption. This study discusses the advantages of the Hill Cipher algorithm in carrying out the encryption and decryption process. By applying this algorithm, it is expected that the message sent will be more secure [8].

## 2. THEORIES

### *2.1 Cryptography*

Cryptography is the art of mathematical techniques related to information security aspects such as confidentiality, data integrity, and authentication [9]. The definition used in the book states that cryptography is the science and art to maintain the confidentiality of messages by encoding them in a form that cannot be understood anymore. This definition may be suitable in the past where cryptography was used for security of essential communications such as communication among the military, diplomats, and spies. Cryptography's current name is more than just privacy, but also for data integrity, authentication, and non-repudiation purposes. Encryption is part of cryptography and is an essential thing so that the security of the data sent can be kept confidential. Encryption can be interpreted by a cipher or code, where the plaintext is converted into separate codes according to the method agreed on by both parties, both the message sender and the recipient of the message. Decryption is a reverse process of encryption that is returning passwords or information that has been traced to the form of the original file using a key or code [10]. Cryptography requires keys in the process of encryption and decryption. The key has two types, symmetrical and asymmetrical. Symmetric keys are the keys used in encryption and decryption are the same while asymmetric keys have different keys when encryption and decryption [11]–[13].

### *2.2 Hill Cipher*

Hill Cipher which is a Polyalphabetic Cipher can be categorized as a Block Cipher because the text to be processed will be divided into blocks of a certain size [14]. Each character in one block will influence other characters in the encryption and decryption process so that the same characters are not mapped into the same characters. This cryptographic technique uses a square matrix as a key used for encryption and decryption. Lester S. Hill created hill

Cipher in 1929 [15]. Hill Cipher does not replace each alphabet in the same plaintext with the same alphabet in the ciphertext because it uses matrix multiplication by encryption and decryption. Hill Cipher includes classic cryptographic algorithms that are very difficult to solve by cryptanalysts if done only by knowing the ciphertext file. However, this technique can be solved quite easily if the cryptanalyst has a ciphertext file and a piece of plaintext file [16]. This cryptanalysis technique is called a known-plaintext attack.

## 3. METHODOLOGY:

The encryption process on Hill Cipher is done per plaintext block. The block size is the same as the size of the key matrix. Before dividing the text into rows of blocks, the plaintext is converted into numbers by referring to the ASCII table. Explanation of the Hill Cipher algorithm can be simplified in this way. Let K be a key matrix with the order of 3 x 3. Then the equation can be obtained to produce the ciphertext as follows:

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{22} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} Mod\ 256$$

The decryption process on Hill Cipher is the same as the encryption process. However, the key matrix must be inversed first. The inverse calculation of a 3 x 3 matrix is described in the following steps.

- Look for key matrix determinants using Sarrus rules

$$\det(K) = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \\ K_{31} & K_{32} \end{bmatrix}$$

$$\det(k) = ((\mathrm{K11} * \mathrm{K22} * \mathrm{K33}) + (\mathrm{K12} * \mathrm{K23} * \mathrm{K31}) + \mathrm{K13} * \mathrm{K21} * \mathrm{K32})) - ((\mathrm{K31} * \mathrm{K22} * \mathrm{K13}) + (\mathrm{K32} * \mathrm{K23} * \mathrm{K11}) + (\mathrm{K33} * \mathrm{K21} * \mathrm{K12}))$$

- Look for determinants of $K^{-1}$

$$(X * Y) mod\ Z = 1$$

where $0 \leq Y \leq Z - 1$
X = Determinants
Y = Determinants of $K^{-1}$
Z = 256

- Look for a minor from the key matrix. If the elements in the i-row and the j-column of the K matrix are deleted, then there will be a square matrix of order 2. The determinant of the square matrix of order two is called the minor of the determinant of the matrix K, denoted by $|M_{ij}|$.

- Look for key matrix cofactors. If $|M_{ij}|$ is a minor Kij of the matrix K, then form (-1) i + j $|M_{ij}|$ is called the cofactor of Kij. Cij symbolizes the cofactor of Kij. So, the $K_{ij}$ cofactor can be determined by the formula Cij = (-1) i + j $|M_{ij}|$.

- Look for adjoin key matrices. Whereas for adjoin matrix K is the transpose of the matrix K.

$$\text{adj K} = \begin{bmatrix} \mathrm{K}_{11} & \mathrm{K}_{21} & \mathrm{K}_{31} \\ \mathrm{K}_{12} & \mathrm{K}_{22} & \mathrm{K}_{32} \\ \mathrm{K}_{13} & \mathrm{K}_{23} & \mathrm{K}_{33} \end{bmatrix}$$

- Look for the key matrix inverse. To find the inverse of this matrix, the following equation is used.

$$K^{-1} = \frac{1}{\det K}\ adj\ K$$

$$K^{-1} = (det\ K^{-1})\ adj\ K$$

## 4. RESULT AND DISCUSSION:

The results of system testing need to be done to determine the value of the benefits of the Hill Cipher algorithm. For implementation, the readiness of the resources that will be used is needed, both regarding hardware and software, the translation of which will be described below. The encryption process on Hill Cipher is done per plaintext block. The block size is the same as the size of the key matrix. Before dividing the text into rows of blocks, the plaintext is converted into numbers by referring to the ASCII table.

Plaintext = sitirosmiyati2@gmail.com

Key = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix}$

C1 = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix} \begin{bmatrix} 115 \\ 105 \\ 116 \end{bmatrix} = \begin{bmatrix} 47577 \\ 30422 \\ 59835 \end{bmatrix} mod 256 = \begin{bmatrix} 217 \\ 214 \\ 187 \end{bmatrix}$

C2 = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix} \begin{bmatrix} 105 \\ 114 \\ 111 \end{bmatrix} = \begin{bmatrix} 48717 \\ 30243 \\ 58071 \end{bmatrix} mod 256 = \begin{bmatrix} 77 \\ 35 \\ 215 \end{bmatrix}$

C3 = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix} \begin{bmatrix} 115 \\ 109 \\ 115 \end{bmatrix} = \begin{bmatrix} 46535 \\ 29366 \\ 58836 \end{bmatrix} mod 256 = \begin{bmatrix} 199 \\ 182 \\ 212 \end{bmatrix}$

C4 = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix} \begin{bmatrix} 121 \\ 97 \\ 116 \end{bmatrix} = \begin{bmatrix} 45723 \\ 29876 \\ 60071 \end{bmatrix} mod 256 = \begin{bmatrix} 155 \\ 180 \\ 167 \end{bmatrix}$

C5 = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix} \begin{bmatrix} 105 \\ 50 \\ 64 \end{bmatrix} = \begin{bmatrix} 24803 \\ 17703 \\ 41720 \end{bmatrix} mod 256 = \begin{bmatrix} 227 \\ 39 \\ 248 \end{bmatrix}$

C6 = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix} \begin{bmatrix} 103 \\ 109 \\ 97 \end{bmatrix} = \begin{bmatrix} 44947 \\ 27818 \\ 54820 \end{bmatrix} mod 256 = \begin{bmatrix} 147 \\ 170 \\ 36 \end{bmatrix}$

C7 = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix} \begin{bmatrix} 105 \\ 108 \\ 46 \end{bmatrix} = \begin{bmatrix} 35447 \\ 21069 \\ 47752 \end{bmatrix} mod 256 = \begin{bmatrix} 119 \\ 77 \\ 136 \end{bmatrix}$

C8 = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix} \begin{bmatrix} 99 \\ 111 \\ 109 \end{bmatrix} = \begin{bmatrix} 47567 \\ 29436 \\ 55906 \end{bmatrix} mod 256 = \begin{bmatrix} 207 \\ 252 \\ 98 \end{bmatrix}$

The decryption process on the Hill cipher is the same as the encryption process. However, the key matrix must be inversed first. The decryption process begins with calculating the inverse of the matrix K. Then the steps of the decryption process are as follows.

Ciphertext = ÙÖ»M#×Ç¶Ô›´§ã'ø“ª$wMˆÏüb

Det (K) = $\begin{bmatrix} 11 & 240 & 182 \\ 41 & 99 & 132 \\ 238 & 149 & 145 \end{bmatrix} \begin{bmatrix} 11 & 240 \\ 41 & 99 \\ 238 & 149 \end{bmatrix}$

= 2878151

Det $K^{-1}$ = 247

$$\text{Cofactor} = \begin{bmatrix} -5313 & 25471 & -17453 \\ -7682 & -41721 & 55481 \\ 13662 & 6010 & -8751 \end{bmatrix}$$

$$\text{Adj (K)} = \begin{bmatrix} -5313 & -7682 & 13662 \\ 25471 & -41721 & 6010 \\ -17453 & 55481 & -8751 \end{bmatrix}$$

$$K^{-1} = 247 \begin{bmatrix} -5313 & -7682 & 13662 \\ 25471 & -41721 & 6010 \\ -17453 & 55481 & -8751 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} -1312311 & -1897454 & 3374514 \\ 6291337 & -10305087 & 1484470 \\ -4310891 & 13703807 & -2161497 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 201 & 18 & 178 \\ 137 & 193 & 182 \\ 149 & 127 & 167 \end{bmatrix}$$

$$P1 = \begin{bmatrix} 201 & 18 & 178 \\ 137 & 193 & 182 \\ 149 & 127 & 167 \end{bmatrix} \begin{vmatrix} 217 \\ 214 \\ 187 \end{vmatrix} = \begin{bmatrix} 80755 \\ 105065 \\ 90740 \end{bmatrix} mod 256 = \begin{bmatrix} 115 \\ 105 \\ 116 \end{bmatrix}$$

$$P2 = \begin{bmatrix} 201 & 18 & 178 \\ 137 & 193 & 182 \\ 149 & 127 & 167 \end{bmatrix} \begin{vmatrix} 77 \\ 35 \\ 215 \end{vmatrix} = \begin{bmatrix} 54377 \\ 56434 \\ 51823 \end{bmatrix} mod 256 = \begin{bmatrix} 105 \\ 114 \\ 111 \end{bmatrix}$$

$$P3 = \begin{bmatrix} 201 & 18 & 178 \\ 137 & 193 & 182 \\ 149 & 127 & 167 \end{bmatrix} \begin{vmatrix} 199 \\ 182 \\ 212 \end{vmatrix} = \begin{bmatrix} 81011 \\ 100937 \\ 88169 \end{bmatrix} mod 256 = \begin{bmatrix} 115 \\ 109 \\ 115 \end{bmatrix}$$

$$P4 = \begin{bmatrix} 201 & 18 & 178 \\ 137 & 193 & 182 \\ 149 & 127 & 167 \end{bmatrix} \begin{vmatrix} 155 \\ 180 \\ 167 \end{vmatrix} = \begin{bmatrix} 64121 \\ 86369 \\ 73844 \end{bmatrix} mod 256 = \begin{bmatrix} 121 \\ 97 \\ 116 \end{bmatrix}$$

$$P5 = \begin{bmatrix} 201 & 18 & 178 \\ 137 & 193 & 182 \\ 149 & 127 & 167 \end{bmatrix} \begin{vmatrix} 227 \\ 39 \\ 248 \end{vmatrix} = \begin{bmatrix} 90473 \\ 83762 \\ 80192 \end{bmatrix} mod 256 = \begin{bmatrix} 105 \\ 50 \\ 64 \end{bmatrix}$$

$$P6 = \begin{bmatrix} 201 & 18 & 178 \\ 137 & 193 & 182 \\ 149 & 127 & 167 \end{bmatrix} \begin{vmatrix} 147 \\ 170 \\ 36 \end{vmatrix} = \begin{bmatrix} 39015 \\ 59501 \\ 49505 \end{bmatrix} mod 256 = \begin{bmatrix} 103 \\ 109 \\ 97 \end{bmatrix}$$

$$P7 = \begin{bmatrix} 201 & 18 & 178 \\ 137 & 193 & 182 \\ 149 & 127 & 167 \end{bmatrix} \begin{vmatrix} 119 \\ 77 \\ 77 \end{vmatrix} = \begin{bmatrix} 49513 \\ 55916 \\ 50222 \end{bmatrix} mod 256 = \begin{bmatrix} 105 \\ 108 \\ 46 \end{bmatrix}$$

$$P8 = \begin{bmatrix} 201 & 18 & 178 \\ 137 & 193 & 182 \\ 149 & 127 & 167 \end{bmatrix} \begin{vmatrix} 207 \\ 252 \\ 98 \end{vmatrix} = \begin{bmatrix} 63587 \\ 94831 \\ 79213 \end{bmatrix} mod 256 = \begin{bmatrix} 99 \\ 111 \\ 109 \end{bmatrix}$$

## 5. CONCLUSION:

Hill Cipher is a classic cryptographic algorithm that is very well used to protect information. This algorithm uses a plaintext matrix relationship with a key. The ciphertext results are very good because they are tied to the characters in the 3 x 3 order matrix. Hill Cipher is very difficult to solve because it has proper mathematical calculations. This algorithm works very quickly in the process of encryption and decryption.

## REFERENCES:

1. H. Ming and S. LiZhong, "A New System Design of Network Invasion Forensics," in *2009 Second International Conference on Computer and Electrical Engineering*, 2009, pp. 596–599.

2. A. Lubis and A. P. U. Siahaan, "Network Forensic Application in General Cases," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 41–44, 2016.
3. M. Iqbal, A. P. U. Siahaan, and R. P. Sundari, "Combination of MD5 and ElGamal in Verifying File Authenticity and Improving Data Security," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 96–101, 2018.
4. M. D. L. Siahaan and A. P. U. Siahaan, "Application of Hill Cipher Algorithm in Securing Text Messages," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 55–59, 2018.
5. A. P. U. Siahaan, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," *Int. J. Adv. Appl. Sci.*, vol. 6, no. 4, pp. 313–318, 2017.
6. W. Fitriani, R. Rahim, B. Oktaviana, and A. P. U. Siahaan, "Vernam Encypted Text in End of File Hiding Steganography Technique," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 7, pp. 214–219, Jul. 2017.
7. A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *Int. J. Sci. Res.*, vol. 5, no. 7, pp. 1149–1152, 2016.
8. F. H. Khan, R. Shams, F. Qazi, and D.-E.-S. Agha, "Hill Cipher Key Generation Algorithm by using Orthogonal Matrix," *Int. J. Innov. Sci. Mod. Eng.*, vol. 3, no. 3, pp. 5–7, 2015.
9. W. Stallings, *Cryptography and Network Security Principles and Practices*, 4th ed. Prentice Hall, 2005.
10. S. S. Sabarish and N. R. Deepthika, "Image Encryption & Decryption by AES 128 BIT Core using FPGA Implementation," *Int. J. Mag. Eng. Technol. Manag. Res.*, vol. 4, no. 1, pp. 375–381, 2017.
11. A. P. U. Siahaan, *How to Code: Advanced Encryption Standard in C#*. Medan: Fakultas Ekonomi Universitas Panca Budi, 2018.
12. Y. Kumar, R. Munjal, and H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," *Int. J. Comput. Sci. Manag. Stud.*, vol. 11, no. 3, pp. 60–63, 2011.
13. A. Putera Utama Siahaan, E. Elviwani, and B. Oktaviana, "Comparative Analysis of RSA and ElGamal Cryptographic Public-key Algorithms," in *Proceedings of the Joint Workshop KO2PI and The 1st International Conference on Advance & Scientific Innovation*, 2018.
14. A. P. U. Siahaan, "Genetic Algorithm in Hill Cipher Encryption," *Am. Int. J. Res. Sci. Technol. Eng. Math.*, vol. 15, no. 1, pp. 84–89, 2016.
15. B. Forouzan, *Cryptography and Network Security*. New York, NY, USA: McGraw-Hill, 2006.
16. A. P. U. Siahaan, "A Fingerprint Pattern Approach to Hill Cipher Implementation."