Application of Hill Cipher Algorithm in Securing Text Messages

[1] **Muhammad Donni Lesmana Siahaan,** [2] **Andysah Putera Utama Siahaan**
Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: [1] donnilesmanasiahaan@gmail.com, [2] andiesiahaan@gmail.com

Abstract: *Computer security aims to help users prevent fraud or detect fraud in an information-based system. The information must be secured to be free from threats. Cryptographic techniques can prevent data theft. One cryptographic algorithm is Hill Cipher. This algorithm is one symmetric cryptography algorithm. The Hill Cipher algorithm uses an m x m sized matrix as the key to encryption and decryption. The fundamental matrix theory used in Hill Cipher is multiplication between matrices and inverses the matrix. Hill Cipher has two types of matrices in general, 2 x 2 and 3 x 3. This study discusses the order 2 x 2. The application of Hill Cipher in text-shaped media is highly recommended because it has fast encryption and decryption speeds. This method is very good at securing data that will be transmitted on an open network.*

Key Words: *Hill Cipher, encryption, decryption, algorithm.*

1. INTRODUCTION:

A computer network is a system consisting of computers that are designed to be able to share resources, communicate, and access information [1]. The purpose of a computer network is to be able to achieve its objectives, every part of the computer network can request and provide services. The party requesting and receiving the service is called the client and who provides and sends the service is called a server. This design is called a client-server system and is used in almost all computer network applications [2]. Securing computer networks or data requires proper techniques. The technique often used in cryptography. Cryptography has many methods that can be used to secure data. One method that is often used is the Hill Cipher algorithm. Hill Cipher is a symmetric key cryptographic algorithm that has several advantages in data encryption [3]. The key matrix is generated using the new binomial coefficient Newton to avoid a key matrix that is not invertible. Encryption process and description using the same key, plaintext can use image or text media. The Hill Cipher algorithm uses an m x m sized matrix as the key to encryption and decryption [4]. The fundamental matrix theory used in Hill Cipher is multiplication between matrices and inverses the matrix. Hill Cipher is the application of modulo arithmetic to cryptography. This cryptographic technique uses a square matrix as the key used to encrypt and decrypt [5]. Security is expected to be guaranteed after applying the Hill Cipher algorithm in the process of sending and receiving data. With this algorithm, users of data delivery services do not need to worry about the dangers of threats that come to hack security systems and steal data.

2. THEORIES:

2.1 Cryptography

Cryptography is the science of encryption techniques where plaintext is encrypted using a secret key so that it becomes ciphertext [6]. This manuscript cannot be solved by someone who does not have a decryption key. Decryption using an agreed key will return the ciphertext to the original data. The probability of retrieving the original text by someone who does not have a decryption key in the not too distant future is very small. The encryption technique used in classical cryptography is symmetric encryption where the decryption key is the same as the encryption key [7]. For public key cryptography, asymmetric encryption techniques are required where the decryption key is not the same as the encryption key [8]. Encryption, decryption and key creation for asymmetric encryption techniques require more intensive computing than symmetric encryption because asymmetric encryption uses very large numbers [9].

2.2 Hill Cipher

Lester S. Hill created hill Cipher in 1929 [10]. This cryptographic technique was created in order to be able to create a cipher that cannot be solved using frequency analysis techniques [11]. Hill Cipher does not replace each of the same alphabets in plaintext with the same alphabet in ciphertext because it uses matrix multiplication by encryption and decryption [12]. 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. Each character in one block will influence the other characters in

the encryption and decryption process so that the same character is not mapped to the same character. Hill Cipher is included in classical cryptographic algorithms which cryptanalysts are very difficult to solve if done only by knowing the ciphertext file only. However, this technique can be solved quite easily if the cryptanalyst has a ciphertext file and a piece of the plaintext file. This cryptanalysis technique is called a known-plaintext attack [13].

The basis of the Hill Cipher technique is modulo arithmetic to the matrix. In its application, Hill Cipher uses matrix multiplication techniques and inverse techniques for matrices. The key to Hill Cipher is the matrix n x n with n is the block size. The K matrix that becomes this key must be an invertible matrix, which has inverse K-1 so that the key must have an inverse because the K-1 matrix is the key used to decrypt [14].

The stages of the Hill Cipher encryption algorithm are as follows [15]:

1. Organize character alphabetically with numeric A → 1, B → 2, ..., Z → 26 or in ASCII (256 characters)
2. Create a key matrix measuring m x m

$$K_{mxm} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

3. Matrix K is an invertible matrix that has multiplicative inverse K^{-1} so that $K.\ K^{-1} = 1$
4. Plaintext P = p1 p2 ... pn, blocked with the same size as the row or column column K

$$P_{qxm} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ p_{q1} & p_{q2} & \cdots & p_{qm} \end{bmatrix}$$

5. Transpose matrix P and became

$$P^{t}_{mxq} = \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{1q} \\ p_{12} & p_{22} & \cdots & p_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1m} & p_{2m} & \cdots & p_{qm} \end{bmatrix}$$

6. Multiply matrix K with transposed P in modulo 26 or 256

$$C^{t} = K_{mxm} P^{t}_{mxq}$$

$$C^{t} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix} \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{1q} \\ p_{12} & p_{22} & \cdots & p_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1m} & p_{2m} & \cdots & p_{qm} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{21} & \cdots & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ c_{1q} & c_{2q} & \cdots & c_{mq} \end{bmatrix}$$

7. Then transpose to

$$C = (C^{t})^{t} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1q} \\ c_{21} & c_{22} & \cdots & c_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mq} \end{bmatrix}$$

8. Change the result of step 7 into the alphabet using alphabetical correspondence with numeric in step 1 to obtain the ciphertext

3. RESULT AND DISCUSSION:

In this section, the Hill Cipher algorithm is tested. 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 first converted to ASCII. The following illustration will explain how the Hill Cipher algorithm performs the encryption and decryption process of the given plaintext.

$$\text{Plaintext} = \text{HILL CIPHERX}$$
$$= [72, 73, 76, 76, 32, 67, 73, 80, 72, 69, 82, 88]$$

$$\text{Key} = \begin{bmatrix} 56 & 27 \\ 145 & 196 \end{bmatrix}$$

$$\text{Determinant} = (56 * 196) - (27 * 145)$$
$$= 7061$$

$$\text{Inverse Key} = \begin{bmatrix} 180 & 17 \\ 243 & 88 \end{bmatrix}$$

The encryption calculation:

$$\text{Ciphertext 1} = \begin{bmatrix} 56 & 27 \\ 145 & 196 \end{bmatrix}\begin{bmatrix} 72 \\ 73 \end{bmatrix}$$

$$= \begin{bmatrix} 115 \\ 172 \end{bmatrix}$$

$$\text{Ciphertext 2} = \begin{bmatrix} 56 & 27 \\ 145 & 196 \end{bmatrix}\begin{bmatrix} 76 \\ 76 \end{bmatrix}$$

$$= \begin{bmatrix} 164 \\ 60 \end{bmatrix}$$

$$\text{Ciphertext 3} = \begin{bmatrix} 56 & 27 \\ 145 & 196 \end{bmatrix}\begin{bmatrix} 32 \\ 67 \end{bmatrix}$$

$$= \begin{bmatrix} 17 \\ 108 \end{bmatrix}$$

$$\text{Ciphertext 4} = \begin{bmatrix} 56 & 27 \\ 145 & 196 \end{bmatrix}\begin{bmatrix} 73 \\ 80 \end{bmatrix}$$

$$= \begin{bmatrix} 104 \\ 153 \end{bmatrix}$$

$$\text{Ciphertext 5} = \begin{bmatrix} 56 & 27 \\ 145 & 196 \end{bmatrix}\begin{bmatrix} 72 \\ 69 \end{bmatrix}$$

$$= \begin{bmatrix} 7 \\ 156 \end{bmatrix}$$

$$\text{Ciphertext 6} = \begin{bmatrix} 56 & 27 \\ 145 & 196 \end{bmatrix}\begin{bmatrix} 82 \\ 88 \end{bmatrix}$$

$$= \begin{bmatrix} 56 \\ 210 \end{bmatrix}$$

$$\text{Ciphertext} = [115, 172, 164, 60, 17, 108, 104, 153, 7, 156, 56, 210]$$
$$= \text{s¬¤<\_lh□\_□8Ò}$$

The decryption calculation:

$$\text{Plaintext 1} = \begin{bmatrix}180 & 17\\ 243 & 88\end{bmatrix}\begin{bmatrix}115\\ 172\end{bmatrix}$$

$$= \begin{bmatrix}72\\ 73\end{bmatrix}$$

$$\text{Plaintext 2} = \begin{bmatrix}180 & 17\\ 243 & 88\end{bmatrix}\begin{bmatrix}164\\ 60\end{bmatrix}$$

$$= \begin{bmatrix}76\\ 76\end{bmatrix}$$

$$\text{Plaintext 3} = \begin{bmatrix}180 & 17\\ 243 & 88\end{bmatrix}\begin{bmatrix}17\\ 108\end{bmatrix}$$

$$= \begin{bmatrix}32\\ 67\end{bmatrix}$$

$$\text{Plaintext 4} = \begin{bmatrix}180 & 17\\ 243 & 88\end{bmatrix}\begin{bmatrix}104\\ 153\end{bmatrix}$$

$$= \begin{bmatrix}73\\ 80\end{bmatrix}$$

$$\text{Plaintext 5} = \begin{bmatrix}180 & 17\\ 243 & 88\end{bmatrix}\begin{bmatrix}7\\ 156\end{bmatrix}$$

$$= \begin{bmatrix}72\\ 69\end{bmatrix}$$

$$\text{Plaintext 6} = \begin{bmatrix}180 & 17\\ 243 & 88\end{bmatrix}\begin{bmatrix}56\\ 210\end{bmatrix}$$

$$= \begin{bmatrix}82\\ 88\end{bmatrix}$$

$$\text{Plaintext} = [72, 73, 76, 76, 32, 67, 73, 80, 72, 69, 82, 88]$$
$$= \text{HILL CIPHERX}$$

After testing the Hill Cipher algorithm against the plaintext "HILL CIPHERX," it can be seen that the ciphertext generated through the encryption process can be returned to plaintext correctly without losing a single character. With this, the Hill Cipher algorithm works well with the use of text-based messages.

4. CONCLUSION:

Hill Cipher is a classic cryptographic algorithm that is very strong regarding its security. The Hill Cipher key matrix must be an invertible matrix. The bigger a key matrix, the stronger the security aspect. This algorithm is strong in dealing with ciphertext-only attacks but is weak if attacked with known-plaintext attacks. The thing that needs to be guarded against this algorithm is the key must be confidential. If the key falls to an irresponsible person, then inverse modulo can determine the key with a series of mathematical calculations.

REFERENCES:

1. H. Ming dan S. LiZhong, “A New System Design of Network Invasion Forensics,” in *2009 Second International Conference on Computer and Electrical Engineering*, 2009, hal. 596–599.
2. A. Lubis dan A. P. U. Siahaan, “Network Forensic Application in General Cases,” *IOSR J. Comput. Eng.*, vol. 18, no. 6, hal. 41–44, 2016.
3. A. P. U. Siahaan, “Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm,” *Int. J. Adv. Appl. Sci.*, vol.

6, no. 4, hal. 313–318, 2017.
4. F. H. Khan, R. Shams, F. Qazi, dan D.-E.-S. Agha, "Hill Cipher Key Generation Algorithm by using Orthogonal Matrix," *Int. J. Innov. Sci. Mod. Eng.*, vol. 3, no. 3, hal. 5–7, 2015.
5. A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *Int. J. Sci. Res.*, vol. 5, no. 7, hal. 1149–1152, 2016.
6. W. Stallings, *Cryptography and Network Security Principles and Practices*, 4th ed. Prentice Hall, 2005.
7. A. P. U. Siahaan, *How to Code: Advanced Encryption Standard in C#*. Medan: Fakultas Ekonomi Universitas Panca Budi, 2018.
8. A. Putera Utama Siahaan, E. Elviwani, dan 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.
9. Y. Kumar, R. Munjal, dan H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," *Int. J. Comput. Sci. Manag. Stud.*, vol. 11, no. 3, hal. 60–63, 2011.
10. B. Forouzan, *Cryptography and Network Security*. New York, NY, USA: McGraw-Hill, 2006.
11. A. P. U. Siahaan, "Genetic Algorithm in Hill Cipher Encryption," *Am. Int. J. Res. Sci. Technol. Eng. Math.*, vol. 15, no. 1, hal. 84–89, 2016.
12. Hasdiana, "Hill Cipher pada Skema Shamir's Three Pass Protocol," Universitas Sumatera Utara, 2015.
13. H. Anton dan C. Rorres, *Elementary Linear Algebra*. John Wiley & Sons, 2011.
14. A. A. Abdullah, R. Khalaf, dan M. Riza, "A Realizable Quantum Three-Pass Protocol Authentication Based on Hill-Cipher Algorithm," *Math. Probl. Eng.*, vol. 2015, hal. 1–6, 2015.
15. M. Khoerudin, "Algoritma Hill Cipher (Sandi Hill)," 2015. [Daring]. Tersedia pada: https://muamalkhoerudin.wordpress.com/2015/03/22/algoritma-hill-cipher-sandi-hill/. [Diakses: 01-Okt-2018].