HILL CIPHER ON SHAMIR'S THREE PASS PROTOCOL

Hasdiana¹⁾, Muhammad Zarlis²⁾, Rahmat Widia Sembiring³⁾, Jamaludin¹⁾

¹⁾Program Studi S2 Teknik Informatika USU, ²⁾Fasilkom TI USU, ³⁾Politeknik Negeri Medan

ABSTRACT

In this study the authors use the scheme of Shamir's Three Pass Protocol for Hill Cipher operation. Scheme of Shamir's Three Pass Protocol is an attractive scheme that allows senders and receivers to communicate without the key exchange. Hill Cipher is chosen because of the key-shaped matrix, which is expected to complicate the various techniques of cryptanalyst. The results of this study indicate that the weakness of the scheme of Shamir's Three Pass Protocol for XOR operation is not fully valid if it is used for Hill Cipher operations. Cryptanalyst can utilize only the third ciphertext that invertible. Matrix transpose techniques in the ciphertext aims to difficulties in solving this algorithm. The original ciphertext generated in each process is different from the transmitted ciphertext. The level of difficulty increases due to the use of larger key matrix. The amount of time required for the execution of the program depends on the length of the plaintext and the value of the matrix element. Plaintext has the same length produce different execution time depending on the value of the key elements of the matrix used.

Keyword: Cryptography, Shamir's Three Pass Protocol, Hill Cipher

1. INTRODUCTION

Shamir's Three Pass Protocol is a scheme that could build communication without the key exchanges. It is because the scheme allow the sender and receiver have their own secrets key. It is called as Three Pass because it should be conducted in three stages of message exchanges. In other words Shamir's Three Pass Protocol is the way to send a message in the message box to the receiver by using two padlocks, but without sharing the key to open the padlock. The use of this scheme can cover the weakness of symmetric-key cryptography, in particular in terms of key secrecy. However, the scheme have a weakness when it is used in the operation of XOR (exclusive-OR). If the cryptanalyst knows or can record the messages exchanges between the sender and the receiver, the cryptanalyst can get back the original message even without knowing the secret key [1].

Based on the principle of Kerckhoff that we should always assume the cryptanalyst knows the cryptographic algorithm which is used, so that the only security of cryptography lies in key [4]. Authors interested in doing research using the scheme of Shamir's Three Pass Protocol for Hill Cipher operation. Hill cipher algorithm is chosen because key-shaped matrix. The use of this algorithm is expected to complicate the various cryptanalyst techniques available. The author also wanted to test whether the weakness of Shamir's Three Pass Protocol used in the XOR operational so applies to operations of Hill Cipher.

Hill Cipher itself is an application of modulo arithmetic in cryptography. It makes Hill Cipher intractable. The technique of this cryptographic is using a square matrix as a key and multiplication matrix as the base of

encryption and decryption. Cipher (code) that have been obtained can not be solved using frequency analysis techniques. Hill cipher is a polygraphic cipher (dividing the original message into groups) that can increase the speed and resistant to frequency analysis attacks [5]. Hill Cipher is classical cryptography that difficult to solve by cryptanalyst if it done by knowing the ciphertext file only. Hill Cipher resistant to ciphertext-only attack, but can be solved by cryptanalysis techniques of known-plaintext attack [7]. It is a cryptanalysis technique in which the cryptanalyst have ciphertext file and pieces of plaintext files. Nevertheless, the cryptanalysis technique of known-plaintext attack can be complicated by enlarging the size of the key matrix [7].

2. MATERIAL AND METHODS

2.1 Hill Cipher Algorithm

Hill Cipher was created by Lester Hillin 1929 [6]. Plaintext on the Hill Cipher Algorithm is grouped into blocks of matrix plaintext. Size of matriks might be (2×1) , (3×1) , $(...)$, $(n \times 1)$. Message is substituted into numeric form $A=0$, $B=1$, and $Z=25$. The number of blocks of matrix are adapted to the length of the encrypted plaintext.

Hill Cipher is using the technique of matrix multiplication and matrix inverse. Keys in Hill Cipher is measuring $n \times n$ matrix where n is the block size [7]. Keys that are used in Hill Cipher algorithm should have inverse because K^{-1} is the decryption key [3]. A square of matrix is invertible if and only if the determinant of the matrix $\neq 0$ (Krantz, 2009) and the determinant of the matrix $\gcd = 1$ [3]. Process of encryption and decryption in the Hill Cipher algorithm can be obtained by the following equation: [7]

$$C \equiv K \cdot P \pmod{26} \text{ dan } P \equiv K^{-1} \cdot C \pmod{26}$$

C =Ciphertext, K =Encryption Key of Hill Cipher(matrix form), K^{-1} =Decryption key of Hill Cipher (matrix invers) and P = Plainteks.

2.2 Shamir's Three-Pass Protocol

Shamir's Three Pass Protocol was first developed by Adi Shamir in about 1980. The basic concept of Shamir's Three Pass Protocol is that each entity has a private encryption and decryption key. Sender is Alice and the receiver is Bob. Shamir's Three Pass Protocol works in three stages. First Alice encrypt a message with her key and sends the encrypted message to Bob. The next stage Bob encrypt that message by his key and sends it back to Alice. The final stage, Alice decrypt the second message with her decryption key. Then Alice sent back to Bob. Finally, Bob can open the message with his decryption key. Between Alice and Bob does not occur the key exchange so that key secrecy still save.

2.3 Observed Variables

The observed variables in this study was text messages in string. It start from the letters of A through Z are converted into numbers from 0 to 25. It is grouped into blocks in square of matrix 3×3 .

2.4 Methods

This study is using Hill Cipher algorithm on Shamir's Three Pass Protocol scheme.

Figure1. Hill Cipher on Shamir's Three Pass Protocol Framework

The figure above explains that the message is secured using the Hillcipher algorithm, while the process of sending a message is using Shamir's Three Pass Protocol scheme. The process of messages exchange run for three times. The common Hill cipher algorithm is changing plaintext into the blocks of matrix measuring 1x2 or 2x1. It is using block of key in square matrix [3]. This study uses block of message and block of key in square matrix of 3x3. Ciphertext position is converted into different form from the original.

2.5 Encryption

This process starts from message which is added the private key of Alice. The position of ciphertext is changed and sent to Bob. The second encryption process encrypted ciphertext-1 and produce the ciphertext-2. Before performing the second encryption, ciphertext-1 is restored to the start position with the assumption that Alice and Bob have to know the techniques of position change. The available ciphertext-2 is sent back to Alice. When Alice received ciphertext-2, the encryption process is complete. However, the position of the ciphertext-2 is also restored to original form before it sent back to Alice.

2.6 Decryption

This process aims to unlock the first encryption. The decryption key is the matrix inverse of encryption key. Ciphertext-2 which is received by Alice encrypted with her decryption key. The first decryption produces ciphertext-3. Its position is changed with the same techniques before being sent to Bob. In the second process of decryption, ciphertext-3 decrypted and produce plaintext. Before performing a second decryption, the ciphertext-3 position is returned first to the starting position. This process is the end process of sending message. Ciphertext has been successfully converted into plaintext through three (3) times process of sending messages.

Figure2. The Flowchart of Hill Cipher On Shamir's Three Pass Protocol

3. RESULT AND DISCUSSIONS

3.1 Encryption Key And Decryption Key

Key A dan Key B is 3 x 3 square of matrix. Key KA^{-1} and Key KB^{-1} is matrix invers of Key A dan Key B.

$$KA = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{ and } KA^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$KB = \begin{pmatrix} 17 & 5 & 20 \\ 23 & 9 & 3 \\ 11 & 2 & 12 \end{pmatrix} \text{ and } KB^{-1} = \begin{pmatrix} 10 & 22 & 19 \\ 19 & 2 & 9 \\ 5 & 25 & 18 \end{pmatrix}$$

3.2 Encryption

To produce the first ciphertext, Alice encrypt the blocks of available plaintext by using the key KA. Encryption is done in the following way:

$$C_1 = P_i \times KA$$

$$= \begin{pmatrix} 5 & 0 & 18 \\ 8 & 11 & 10 \\ 14 & 12 & 25 \end{pmatrix} \times \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} = \begin{pmatrix} 121 & 121 & 367 \\ 387 & 354 & 461 \\ 540 & 504 & 797 \end{pmatrix} \text{mod } 26$$

$$= \begin{pmatrix} 17 & 17 & 3 \\ 23 & 16 & 19 \\ 20 & 10 & 17 \end{pmatrix} \text{transpose} = \begin{pmatrix} 17 & 23 & 20 \\ 17 & 16 & 10 \\ 3 & 19 & 17 \end{pmatrix}$$

Cipherteks-1: 17 23 20 17 16 10 3 19 17
 R X U R Q K D T R

$$\begin{aligned} C_2 &= KB \times C_1 \\ &= \begin{pmatrix} 17 & 5 & 20 \\ 23 & 9 & 3 \\ 11 & 2 & 12 \end{pmatrix} \times \begin{pmatrix} 17 & 17 & 3 \\ 23 & 16 & 19 \\ 20 & 10 & 17 \end{pmatrix} = \begin{pmatrix} 804 & 569 & 486 \\ 658 & 11 & 291 \\ 473 & 399 & 275 \end{pmatrix} \text{mod } 26 \\ &= \begin{pmatrix} 24 & 23 & 18 \\ 8 & 19 & 5 \\ 5 & 1 & 15 \end{pmatrix} \text{transpose} = \begin{pmatrix} 24 & 8 & 5 \\ 23 & 19 & 1 \\ 18 & 5 & 15 \end{pmatrix} \end{aligned}$$

Cipherteks -2: 24 8 5 23 19 1 18 5 15
 Y I F X T B S F P

3.3Decryption

To produce the third ciphertext, Alice decrypt ciphertext-2 (C_2) by using the Decryption key KA^{-1} . Decryption is done in the following way:

$$\begin{aligned} C_3 &= C_2 \times KA^{-1} \\ &= \begin{pmatrix} 24 & 23 & 18 \\ 8 & 19 & 5 \\ 5 & 1 & 15 \end{pmatrix} \times \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 873 & 607 & 804 \\ 437 & 395 & 319 \\ 395 & 62 & 336 \end{pmatrix} \text{mod } 26 \\ &= \begin{pmatrix} 15 & 9 & 24 \\ 21 & 5 & 7 \\ 5 & 10 & 24 \end{pmatrix} \text{transpose} = \begin{pmatrix} 15 & 21 & 5 \\ 9 & 5 & 10 \\ 24 & 7 & 24 \end{pmatrix} \end{aligned}$$

Cipherteks -3 : 15 21 5 9 5 10 24 7 24
 P V F J F K Y H Y

$$\begin{aligned} C_4 &= KB^{-1} \times C_3 \\ &= \begin{pmatrix} 10 & 22 & 19 \\ 19 & 2 & 9 \\ 5 & 25 & 18 \end{pmatrix} \times \begin{pmatrix} 15 & 9 & 24 \\ 21 & 5 & 7 \\ 5 & 10 & 24 \end{pmatrix} = \begin{pmatrix} 707 & 390 & 850 \\ 372 & 271 & 686 \\ 690 & 350 & 727 \end{pmatrix} \text{mod } 26 \\ &= \begin{pmatrix} 5 & 0 & 18 \\ 8 & 11 & 10 \\ 14 & 12 & 25 \end{pmatrix} \text{transpose} = \begin{pmatrix} 5 & 8 & 14 \\ 0 & 11 & 12 \\ 18 & 10 & 25 \end{pmatrix} \end{aligned}$$

Plainteks : 5 0 18 8 11 10 14 12 25
 F A S I L K O M Z

3.4 Findings

Research about Three Pass Protocol and XOR algorithm shows us that the Three Pass Protocol has a fatal weakness [1]. Weakness is that if the cryptanalyst can record process of message exchange and knowing the ciphertext-1 to ciphertext-3. Therefore, this study simultaneously test whether the theory which is mentioned above also applies to the hill cipher algorithm. From the analysis of encryption and decryption above, then:

$$C_1 = P \times KA \dots \dots \dots (1)$$

$$C_2 = KB \times C_1 = KB \times (P \times KA) \dots \dots \dots (2)$$

$$C_3 = C_2 \times KA' = KB \times (P \times KA) \times KA' = KB \times P \dots \dots \dots (3)$$

From the equation above, it was found that to get a first encryption key or keys KA specify the inverse of the ciphertext-3, equation is as follow:

$$KA = C_3' \times C_2 = (KB \times P)' \times KB \times (P \times KA) = P^{-1} \times KB^{-1} \times KB \times P \times KA = KA$$

If the encryption key KA has been obtained. So plaintext can also easy to found. This the following steps:

$$P = C_1 \times KA' = (P \times KA) \times KA' = P$$

To prove the equation above, the following analysis is illustrated using the results of encryption and decryption that has been described previously. To get KA, determine the inverse of C_3 first:

$$\begin{aligned} \text{Invers}(C_3) &= \begin{pmatrix} 22 & 22 & 3 \\ 11 & 12 & 5 \\ 19 & 11 & 6 \end{pmatrix} \\ \text{KeyKA} &= C_3' \times C_2 \\ &= \begin{pmatrix} 22 & 22 & 3 \\ 11 & 12 & 5 \\ 19 & 11 & 6 \end{pmatrix} \times \begin{pmatrix} 24 & 23 & 18 \\ 8 & 19 & 5 \\ 5 & 1 & 15 \end{pmatrix} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \\ \text{Plaintext} &= C_1 \times KA' \\ &= \begin{pmatrix} 17 & 17 & 3 \\ 23 & 16 & 19 \\ 20 & 10 & 17 \end{pmatrix} \times \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 5 & 0 & 18 \\ 8 & 11 & 10 \\ 14 & 12 & 25 \end{pmatrix} \\ &= \text{F A S I L K O M Z} \end{aligned}$$

The results of encryption and decryption simulation process by using plaintext Fasilkom successfully performed. Encryption key is the key of A(KA) and key of B(KB). While the decryption key is KA^{-1} and KB^{-1} . The resulting matrix of ciphertext is not the result of actual ciphertext calculation because each form of the ciphertext matrix is converted into different form. By using scheme of Hill Cipher on Shamir's Three Pass Protocol, the weakness of the scheme which is outlined above can be overcome. Cryptanalyst can only solve the encryption key if matrix of available ciphertext is invertible. In this study the authors use the concept of matrix transpose to change the shape of the original ciphertext matrix. The same message length requires a different execution time. It is depend on variations of the matrix Key A and key B during the process of encryption and decryption (Table 1). Different message length also require a different execution time depending on the number of characters during the process of encryption and decryption (Table 2).

Table1. Simulation of Encryption and Decryption

with TheVarious Key			
Variation Key Matriks(3x3)		Plaintext (Number of character)	Execution Time
Matrix A	Matrix B		
[78, 57, 38] [52, 74, 61] [9, 9, 84]	[2, 0, 19] [6, 7, 9] [13, 8, 8]	100	0,26
[3, 89, 54] [66, 3, 50] [2, 71, 65]	[21, 13, 23] [7, 23, 18] [12, 25, 16]	100	0,37
[1, 68, 27] [2, 95, 78] [51, 49, 98]	[25, 4, 9] [1, 6, 0] [8, 3, 9]	100	0,37
[58, 8, 51] [1, 28, 87] [76, 73, 33]	[15, 24, 8] [10, 24, 1] [8, 21, 1]	100	0,24
[70, 85, 5] [18, 90, 71] [67, 52, 92]	[2, 15, 4] [4, 0, 23] [11, 18, 13]	100	0,35

Table2. Simulation of Encryption and Decryption

with the Various Plaintext			
Key Matriks(3x3)		Variation Plaintext (number of character)	Execution Time
Matriks A	Matriks B		
[17, 17, 5] [21, 18, 21] [2, 2, 19]	[17, 5, 23] [23, 9, 3] [11, 2, 12]	20	0,28
[17, 17, 5] [21, 18, 21] [2, 2, 19]	[17, 5, 23] [23, 9, 3] [11, 2, 12]	50	0,37
[17, 17, 5] [21, 18, 21] [2, 2, 19]	[17, 5, 23] [23, 9, 3] [11, 2, 12]	100	0,37
[17, 17, 5] [21, 18, 21] [2, 2, 19]	[17, 5, 23] [23, 9, 3] [11, 2, 12]	150	0,43
[17, 17, 5] [21, 18, 21] [2, 2, 19]	[17, 5, 23] [23, 9, 3] [11, 2, 12]	300	0,9

4. CONCLUSION

Based on the discussion and evaluation of the previous discussion, it can be concluded as follows:

1. The weakness of Shamir's Three Pass Protocol scheme by utilizing the ciphertext is not fully valid because it is supported by using Hill cipher algorithm for encryption and decryption.
2. Cryptanalyst can only formulate the encryption key through invertible ciphertext-3. It is recommended to use a key with a large size.
3. Modification of the ciphertext is using matrix transpose concept so that can complicate the cryptanalyst. The concept can be modified to other various concepts.
4. The amount of time that is required for the program execution depends on the length of the plaintext and the value of the matrix element. Plaintext with the same length can result in different execution times depending on the value of the key elements of the matrix used.

5. REFERENCE

- [1] Kanamori, Y. & Yoo, S. 2009. *Quantum Three Pass Protocol Key Distribution Using Quantum Superposition State*. International Journal of Network Security Application (IJNSA)1(2): 64-70.
- [2] Krantz, Steven G. 2009. *Discrete Mathematics Demystified*. The McGraw-Hill Companies, Inc: New York.
- [3] Mollin, A. R. 2007. *An Introduction to Cryptography*. Second Edition. Taylor & Francis Group. LLC.
- [4] Munir, R. 2006. *Kriptografi*. Informatika Bandung: Bandung.
- [5] Rahman M.N.A, Abidin A.F.A, Yusof MK & Usop N.S.M. 2013. *Cryptografi: A New approach of classical Hill Cipher*. International Journal of Security and its Applications 7(2):179-190.
- [6] Stallings, William. 2003. *Cryptography and Network Security*. Prentice Hall.
- [7] Widyanarko, Arya. 2007. *Studi dan Analisis mengenai Hill Cipher, Teknik Kriptanalisis dan Upaya Penanggulangannya*. Makalah Program Studi Teknik Informatika Institut Teknologi Bandung.