International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Three-Pass Protocol Concept in Hill Cipher Encryption Technique

Andysah Putera Utama Siahaan

Faculty of Computer Science, Universitas Pembangunan Panca Budi
Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia

Abstract: ***Hill Cipher Encryption technique has a square matrix in its calculation. The ciphertext resulted is obtained from the matrix multiplication between plaintext and key. The reality is the sender must send or tell the receiver the key used to encrypt the data before the receiver can decode the ciphertext into the legible message. The listener is able to read the key that flows to the receiver. By knowing the key, the listener will absolutely break the ciphertext and turn into plaintext. Three-Pass Protocol is a way to limit the key being distributed. The sender and receiver have their own keys in hand. They do not need to share each other. This method will improve the security.***

Keywords: Cryptography, Three-Pass Protocol, Hill Cipher, Encryption, Decryption

1. Introduction

The confidential information must be protected from being intercepted [9]. There is a various way to perform the encryption. Hill Cipher is one of the encryption algorithms that uses matrix [8][7]. The smallest matrix of 2x2 can produce the ciphertext by providing key as the determinant. The matrix bigger than 2x2 can be used as well, but the difficulties in finding the inverse matrix gain more too. In Hill Cipher, we can randomly describe the integers for keys beforehand [5][6]. However, sometimes the key provided does not work. It happens when decoding the ciphertext back to plaintext. It is different from the original message. Before using the key, we have to test that it has the right determinant. Moreover, if so, the inverse key will be applied to the ciphertext when decryption is happening. Since we use the key as a password to modify the message, we have to send or give to someone who is responsible for decrypting the message. The key must be distributed, and this moment will be taken by third parties to intercept the known plaintext to be breakable. Three-Pass Protocol is the best way to reduce the gap of interception. On the application of this algorithm, the form of the matrix must be modified. The are several changes of Hill Cipher part to make the both algorithms work together.

2. Theories

The symmetric key is one of the cryptographic systems that uses the same kind of keys in encryption and decryption. Hill Cipher uses the symmetric key in its application. However, the keys used in encryption and decryption are different but same. It happens because the key used in decryption is the inverse of the original key applied when sending plaintext to the receiver [2][3]. The both keys must be correctly calculated for them to generate encrypt and decrypt key pair in encryption and decryption works.

Hill Cipher is an application of modulo arithmetic in cryptography [4]. This cryptographic technique uses the matrix as the vessel of information exchange either on encryption or decryption part. The basic theory of matrix used in Hill Cipher is the multiplication between the matrix and the inverse of the matrix. Hill Cipher is a symmetric key hard to solve because the cryptanalysis techniques such as frequency analysis can not be applied easily to solve this algorithm [2]. Hill cipher is very difficult to solve if cryptologist has only the ciphertext, but it can be solved easily if the cryptologist has a part of the plaintext.

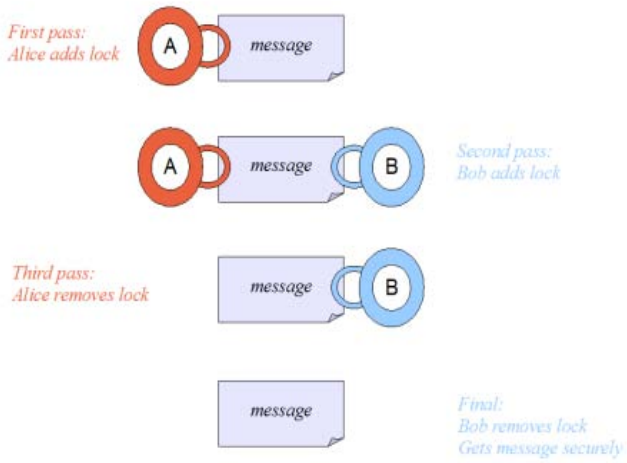

Figure 1: The Three-Pass Protocol scheme

Three-Pass Protocol method is a way to send a message securely from sender to receiver without the need to exchange or distribute encryption keys [1]. In Three-Pass Protocol, the sender encrypts the message using a unique encryption key then they send it to the receiving participant. When the receiver gets the encrypted message, they then encrypt it with their own unique encryption key and send back to the sender. Then the sender decrypts the message with their own key. After this, there is only one level of encryption on the package which is sent to the receiver who decrypts the final layer with their unique decryption key and reads the data. This protocol can only be used if using commutative ciphers or LIFO method. Commutative means that the order of encryption and decryption is interchangeable (Encryption A - Encryption B - Decryption A - Decryption B) [4](Figure 1).

3. Proposed Work

In the application of Three-Pass Protocol in Hill Cipher, the plaintext cannot directly transform to ciphertext and then re-encrypt the message with the second key. If we do this when doing the decryption, the message will not turn back to its original message, it turns to different characters order. We have to modify the encryption block with a square block. It means, when we use a key of a matrix of 2 x 2, the plaintext block will be 2 x 2 as well. It is totally different from the usual Hill Cipher encryption that uses different matrix order.

$$C = \begin{pmatrix} a & b \\ c & d \end{pmatrix} x \begin{pmatrix} p1 & p3 \\ p2 & p4 \end{pmatrix} mod\ TotalCharacter \quad (1)$$

$$D = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} x \begin{pmatrix} c1 & c3 \\ c2 & c4 \end{pmatrix} mod\ TotalCharacter \quad (2)$$

From the formulas above, the encryption and decryption are using the same blocks with the key.

4. Testing and Implementation

In this section, we try to prove the Three-Pass Protocol. Let's take an example below:

Plaintext : ANDY$\begin{pmatrix} 65 & 68 \\ 78 & 89 \end{pmatrix}$

Key 1 : $\begin{pmatrix} 240 & 97 \\ 65 & 163 \end{pmatrix}$

Key 2 : $\begin{pmatrix} 187 & 23 \\ 148 & 223 \end{pmatrix}$

Key 1^{-1} : $\begin{pmatrix} 205 & 145 \\ 113 & 16 \end{pmatrix}$

Key 2^{-1} : $\begin{pmatrix} 55 & 209 \\ 76 & 115 \end{pmatrix}$

Now we prove that the keys provided are invertible.

Key 1 : $\begin{pmatrix} 240 & 97 \\ 65 & 163 \end{pmatrix}$

Determinant : (240 * 163 - 97 * 65)*mod* 256
47 (D ≠ 0*and* D ≠ *Even*)

Key 2 : $\begin{pmatrix} 187 & 23 \\ 148 & 223 \end{pmatrix}$

Determinant : (187 * 223 - 23 * 148) *mod* 256
153 (D ≠ 0 *and* D ≠ *Even*)

Since determinants are not zero or even, we can use the key pair as keys for Hill Cipher.

Encryption 1

Plaintext : $\begin{pmatrix} 65 & 68 \\ 78 & 89 \end{pmatrix}$

Ciphertext 1 : $\begin{pmatrix} 240 & 97 \\ 65 & 163 \end{pmatrix}$ x $\begin{pmatrix} 65 & 68 \\ 78 & 89 \end{pmatrix}$

C1 : (240 * 65 + 97 * 78) *mod* 256
23166 *mod* 256
126

C2 : (65 * 65 + 163 * 78) *mod* 256
16939 *mod* 256
43

C3 : (240 * 68 + 97 * 89) *mod* 256
24953 *mod* 256
121

C4 : (65 * 68 + 163 * 89) *mod* 256
18927 *mod* 256
239

Ciphertext 1 : $\begin{pmatrix} 126 & 121 \\ 43 & 239 \end{pmatrix}^T$

Ciphertext 1^T : $\begin{pmatrix} 126 & 43 \\ 121 & 239 \end{pmatrix}$

Encryption 2

Ciphertext 1^T : $\begin{pmatrix} 126 & 43 \\ 121 & 239 \end{pmatrix}$

Ciphertext 2 : $\begin{pmatrix} 187 & 23 \\ 148 & 223 \end{pmatrix}$ x $\begin{pmatrix} 126 & 43 \\ 121 & 239 \end{pmatrix}$

C1 : (187 * 126 + 23 * 121) *mod* 256
26345*mod* 256
233

C2 : (148 * 126 + 223 * 121) *mod* 256
45631*mod* 256
63

C3 : (187 * 43 + 23 * 239) *mod* 256
13538*mod* 256
226

C4 : (148 * 43 + 223 * 239) *mod* 256
59661*mod* 256
13

Ciphertext 2 : $\begin{pmatrix} 233 & 226 \\ 63 & 13 \end{pmatrix}^T$

Ciphertext 2^T : $\begin{pmatrix} 233 & 63 \\ 226 & 13 \end{pmatrix}$

Ciphertext $2^T$is the final result of the encryption the both methods. And for the decryption, we do the same way as easrlier. We see the explanation below:

Decryption 1

Ciphertext 2^T : $\begin{pmatrix} 233 & 63 \\ 226 & 13 \end{pmatrix}$

Ciphertext 3 $\begin{pmatrix} 205 & 145 \\ 113 & 16 \end{pmatrix}$ x $\begin{pmatrix} 233 & 63 \\ 226 & 13 \end{pmatrix}$

C1 : (205 * 233 + 145 * 226) *mod* 256
80535*mod* 256
151

C2 : (113 * 233 + 16 * 226) *mod* 256
29945*mod* 256
249

C3 : (205 * 63 + 145 * 13) *mod* 256
14800*mod* 256
208

C4 : (113 * 63 + 16 * 13) *mod* 256
7327*mod* 256
159

Ciphertext 3 : $\begin{pmatrix} 151 & 208 \\ 249 & 159 \end{pmatrix}^T$

Ciphertext 3^T : $\begin{pmatrix} 151 & 249 \\ 208 & 159 \end{pmatrix}$

Decryption 2

Ciphertext 3^T : $\begin{pmatrix} 151 & 249 \\ 208 & 159 \end{pmatrix}$

Plaintext : $\begin{pmatrix} 55 & 209 \\ 76 & 115 \end{pmatrix}$ x $\begin{pmatrix} 151 & 249 \\ 208 & 159 \end{pmatrix}$

P1 : (55 * 151 + 209 * 208) *mod* 256
51777 *mod* 256
65

P2 : (76 * 151 + 115 * 208) *mod* 256
35396 *mod* 256
68

P3 : (55 * 249 + 209 * 159) *mod* 256
46926 *mod* 256
78

P4 : (76 * 249 + 115 * 159) *mod* 256
37209 *mod* 256
89

Plaintext : $\begin{pmatrix} 65 & 78 \\ 68 & 89 \end{pmatrix}^T$

Plaintext ^{T} : $\begin{pmatrix} 65 & 68 \\ 78 & 89 \end{pmatrix}$

Plaintext^{T}is the final result of the decryption the both methods.

After calculation, we can see the plaintext is turned into three parts of ciphertexts before finally turned back into plaintext again. Each participant needs to perform two stage of calculation where the sender does the encryption and decryption.For example in Table 1, it shows the complete work of encryption and decryption processes. The sentence is "THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG". There are 40 characters. The PT1 shows the ASCII code of the characters, CT1, CT2 and CT3 is the three-pass protocol processes. The PT2 is the decryption of the ciphertext.

Table 1: Sample of Three-Pass Protocol in Hill Cipher

NO.	PT1	CT1	CT2	CT3	PT2
1	84	228	5	115	84
2	72	179	225	97	72
3	69	220	63	240	69
4	32	135	123	248	32
5	81	198	212	185	81
6	85	24	131	252	85
7	73	11	42	167	73
8	67	179	20	194	67
9	75	253	102	228	75
10	32	228	140	67	32
11	66	169	123	14	66
12	82	246	81	242	82
13	79	30	154	224	79
14	87	34	32	91	87
15	78	213	124	190	78
16	32	186	153	133	32
17	70	151	150	148	70
18	79	72	28	234	79
19	88	162	109	46	88
20	32	72	110	109	32
21	74	197	79	183	74
22	85	251	141	11	85
23	77	142	202	234	77
24	80	95	169	111	80
25	83	181	111	183	83
26	32	187	141	8	32
27	79	129	90	74	79
28	86	149	88	118	86
29	69	9	70	250	69
30	82	92	222	15	82
31	32	7	151	48	32
32	84	96	213	10	84
33	72	39	122	240	72
34	69	68	208	248	69
35	32	216	153	142	32
36	76	96	232	187	76
37	65	69	139	137	65
38	90	255	179	220	90
39	89	155	206	180	89
40	32	163	180	110	32

The use of Three-Pass Protocol on Hill Cipher is very useful way to improve the data security level in the process of sending a message. Besides improving the security, this method also stops distributing keys between sender and receiver. If someone wants to take the information, it will be suspended.In Table 1, we see there are three ciphertext produced. Someone might be intercepting the information. But actually, he does not have the keys since they are not transferred. It is hard to break the hidden information since the key is not provided. But in the conventional method, the key is distributed as well. It really makes the key vulnerable.

5. Conclusion

We concludethat Three-Pass Protocol can be applied in Hill Cipher encryption. It helps the sender to give more protection to their data from being intercepted. The undistributed key system is more secure since the both participants do not have to exchange key when doing this process. Three-Pass Protocol is the best technique to gain the information security more.

References

[1] A. A. Abdullah, R. Khalaf dan M. Riza, "A Realizable Quantum Three-Pass Protocol Authentication," Mathematical Problems in Engineering, 2015.
[2] R. Kumar dan R. C., "Analysis of Diffie Hellman Key Exchange Algorithm with Proposed Key Exchange Algorithm," International Journal of Emerging Trends & Technology in Computer Science, vol. 4, no. 1, pp. 40-43, 2015.
[3] M. Ahmed, B. Sanja, D. Aldiaz, A. Rezaei dan H. Omotunde, "Diffie-Hellman and Its Application in Security Protocols," International Journal of Engineering Science and Innovative Technology, vol. 1, no. 2, pp. 69-73, 2008.
[4] C. Stubbs, "Three-Pass Protocol," 20 November 2013. [Online]. Available: http://asymmetriccryptography.blogspot.co.id/. [Diakses 1 May 2016].
[5] M. N. A. Rahman, A. F. A. Abidin, M. K. Yusof dan N. S. M. Usop, "Cryptography: A New Approach of Classical Hill Cipher," International Journal of Security and Its Applications, vol. 7, no. 2, pp. 179-190, 2013.
[6] S. I. Chowdhury, S. A. M. Shohag dan H. Sahid, "A Secured Message Transaction Approach by Dynamic Hill Cipher Generation and Digest Concatenation," International Journal of Computer Applications, vol. 23, no. 9, pp. 25-31, 2011.
[7] A. A. Khalaf, M. S. A. El-karim dan H. F. A. Hamed, "A Triple Hill Cipher Algorithm Proposed to Increase the Security of Encrypted Binary Data and its Implementation Using FPGA," ICACT Transactions on Advanced Communications Technology, vol. 5, no. 1, pp. 752-757, 2016.
[8] J. Chase dan M. Davis, "Extending the Hill Cipher," 2010.
[9] A. P. U. Siahaan, "RC4 Technique in Visual Cryptography RGB Image Encryption," International Journal of Computer Science and Engineering, vol. 3, no. 7, pp. 1-6, 2016.

Author Profile

Andysah Putera Utama Siahaan was born in Medan, Indonesia, in 1980. He received the S.Kom. degree in computer science from Universitas Pembangunan Panca Budi, Medan, Indonesia, in 2010, and the M.Kom. in computer science as well from the University of Sumatera Utara, Medan, Indonesia, in 2012. In 2010, he joined the Department of Engineering, Universitas Pembangunan Panca Budi, as a Lecturer, and in 2012 became a junior researcher. He is applying for his Ph. D. degree in 2016. He has written in several international journal and conference. He is now active in writing papers and joining conferences.