International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 5, October 2021, pp. 4449~4457
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i5.pp4449-4457

Mixed Hill Cipher methods with triple pass protocol methods

Liqaa Saadi Mezher[1], Ayam Mohsen Abbass[2]
[1]Department of Electrical Engineering, Al-Mustansiriyah University, Baghdad, Iraq
[2]Department of Computer Engineering, Al-Mustansiriyah University, Baghdad, Iraq

Article Info

Article history:

Received Aug 19, 2020
Revised Apr 4, 2021
Accepted Apr 11, 2021

Keywords:

Cipher text
Hill Cipher
Key
No key-exchange
Plain text
Triple pass protocol

ABSTRACT

Hill Cipher is a reimbursement coding system that converts specific textual content codes into numbers and does no longer exchange the location of fixed symbols. The symbol modifications simplest in step with the English letter table inclusive of (26) characters handiest. An encoded Hill Cipher algorithm was used that multiplication the square matrix of the apparent text with a non-public key and then combined it with the Triple Pass Protocol method used to repeat the encryption three times without relying on a personal key. Also, you could decode the code and go back it to the express textual content. The cause of mixing algorithms is to cozy the message without any key change among the sender and the recipient.

Corresponding Author:

Liqaa Saadi Mezher
Department of Electrical Engineering
AL Mustansiryihya University, Baghdad, Iraq
Email: iqa35@uomustansiriyah.edu.iq

1. INTRODUCTION

The three pass protocol is a piece scheme that permits two people to exchange messages without replacing keys. Use of three-pass protocol scheme to not needed key trade manner. The method, that's used, is referred to as Three-Pass Protocol. This protocol permits message transport technique without the key alternate. Therefore, the sending messages process can reach the receiver appropriately without worry of key leakage [1]-[4].

Three-pass protocol is a framework that lets in the sender to send encrypted messages to the recipient without need to distribute the sender's key to the receiver [5]. This system is referred to as Three-Pass Protocol due to the fact the sender and receiver perform three exchange stages to encrypt the message. The primary concept of three-pass protocol is that each party has a private encryption key and a personal decryption key. Each parties independently use the key to encrypt messages and to decrypt messages [6]-[9]. Triple pass protocol is a piece scheme that allows two humans to alternate messages without replacing keys [10].

Hill Cipher is likewise referred to as that the substitution ciphers system [11]-[14]. It is the systems that replace express text symbols with different symbols to attain the encrypted text and the locations of those symbols do not exchange, but as an alternative the symbols themselves are converting and represented the plain text of the letter matrix based on length of message of the same measurement and multiplication the plain text with security key the mod (26) due to the fact the letters in English is same (26) letters this method additionally referred to as linear transform [15]-[19]. The Hill Cipher makes use of the same algorithm for encryption and decryption however used safety key in encryption and inverse key to decryption.

This paper is organize as follows: In segment 2, we gift triple pass protocol method. In section three, Hill Cipher text method supplied. In segment 4, TPP based on Hill Cipher algorithms. In section five, numerous examples were implemented to represent the TTP with Hill Cipher text. In the end, conclusions are supplied in phase 6.

2. THREE PASS PROTOCOL (TRIPLE PASS PROTOCOL) METHOD

This technique is called the three-pass protocol due to the fact the sender and receiver exchange three encrypted messages. It turned into advanced by the scientist Adi Shamir circa 1980 [20]-[22], the flow chart of this technique as shown in Figure 1 [2]. This method is used to encrypt the message and ship it accurately without the need for any key so that each celebration has a private key to encrypt the message and a private key decrypt the message because of this the two events use their keys independently (but the protocol call for the sender and receiver to have two private keys for encrypting and decrypting messages). The systems of three pass protocol as shown in Figure 2 [1].

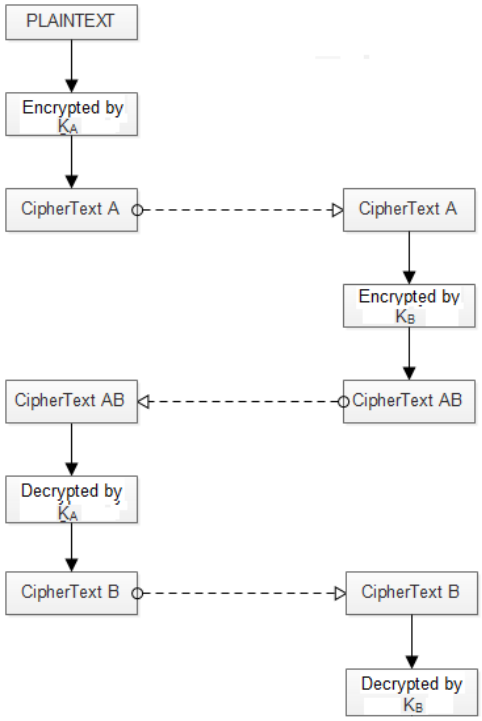

Figure 1. Flow chart of three pass protocol

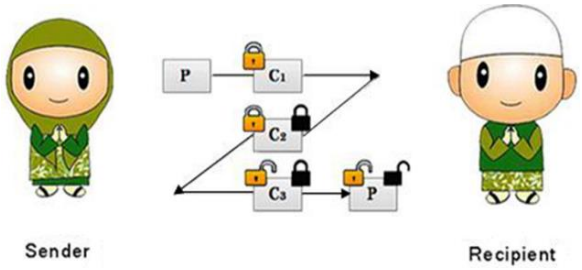

Figure 2. The system of triple pass protocol

3. HILL CIPHER TEXT METHOD

It's far the systems that replace express textual content symbols with different symbols to reap the encrypted textual content and the locations of those symbols do now not change, but instead the symbols themselves are converting. In her work, she is based on linear algebra, developed with the aid of Lester S Hill in 1929 [7], as shown in Figure 3. It is one of the compensatory era methods used to encode letters and convert them to numbers, as it depends on the table of English letters inclusive of (26) letters starting from letter A and ending with the letter Z, according to Table 1.

Additionally in this method the secret key's used within the coding system and is arranged in the form of a square matrix (range of rows=range of columns) and the mathematical equation is used (1).

$$C = K.P \ mod \ (26) \quad (1)$$

Inside the case of decryption, we take the inverse of the key [23]-[25] taking the final result from the coding process, and the use of the mathematical (2).

$$P = K^{-1}.C \ mod \ (26) \quad (2)$$

And extracting the plain text and then after that the numbers are changed with the aid of the letters in step with Table 2.

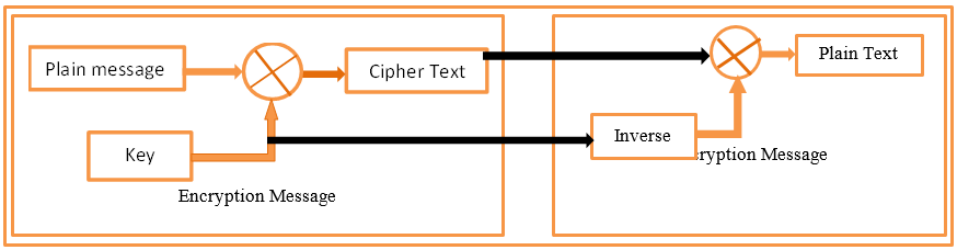

Figure 3. Encryption and decryption of Hill Cipher

Table 1. Convert letter to number

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2. Convert number to letter

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

4. TPP BASED ON HILL CIPHER ALGORITHMS

- Constitute the plain text to square matrix (N*N).
- Convert letter plain text matrix to number plain text matrix relied on the Table 1, use the square key.
- Follow the encryption (1) to number plain text matrix and the use of Hill Cipher text.
- Repeat step (3), to apply triple pass protocol (TTP) to discover the cipher text.
- Convert Key to inverse Key.
- Apply the Decryption (2), the use of the final result of cipher textual content with inverse textual content.
- Repeat step (6), to apply triple pass protocol (TTP) to find the plain text.
- Convert the number plain text matrix to letter plain text matrix depended on the Table 2, to find the original plain text.

5. CASE STUDY

Several examples have been carried out to symbolize the TTP with Hill Cipher text. The calculation system usage of the mixture of the two algorithms inside the three pass protocol scheme is as follows: For example, sender desires to encrypt plain text which with the aid of the usage of Hill Cipher.

a. Example 1

In this case, the plain text = (HELP) and the Key= [1 2; 0 3]:

Constitute the plain text to square matrix (N*N), in which N=2.

$$Plain\ text = \begin{bmatrix} H & L \\ E & P \end{bmatrix}$$

Convert the plain text from the letter matrix to number matrix using Table 1.

$$P = \begin{bmatrix} H & L \\ E & P \end{bmatrix} = \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix}$$

$$\text{Key} = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

Encryption the plain text by using (1).

$$C_1 = K.P \ mod\ 26$$

$$C_1 = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}.\begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix} mod\ 26$$

$$C_1 = \begin{bmatrix} 15 & 41 \\ 12 & 45 \end{bmatrix} mod\ 26 = \begin{bmatrix} 15 & 15 \\ 12 & 19 \end{bmatrix}.$$

$$C_2 = K.C_1\ mod\ 26$$

$$C_2 = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}.\begin{bmatrix} 15 & 15 \\ 12 & 19 \end{bmatrix} mod\ 26$$

$$C_2 = \begin{bmatrix} 39 & 53 \\ 36 & 57 \end{bmatrix} mod\ 26 = \begin{bmatrix} 13 & 1 \\ 10 & 5 \end{bmatrix}$$

$$C_3 = K.C_2\ mod\ 26$$

$$C_3 = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}.\begin{bmatrix} 13 & 1 \\ 10 & 5 \end{bmatrix} mod\ 26$$

$$C_3 = \begin{bmatrix} 33 & 11 \\ 30 & 15 \end{bmatrix} mod\ 26 = \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix}$$

Decryption the cipher text to plain text by using key inverse and the C_3 based on (2):

$$Key^{-1} = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}$$

$$P_1 = K^{-1}.C_3\ mod\ 26$$

$$P_1 = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}.\begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix} mod\ 26$$

$$P_1 = \begin{bmatrix} 39 & 131 \\ 36 & 135 \end{bmatrix} mod\ 26 = \begin{bmatrix} 13 & 1 \\ 10 & 5 \end{bmatrix}.$$

$$P_2 = K^{-1}.P_1\ mod\ 26$$

$$P_2 = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}.\begin{bmatrix} 13 & 1 \\ 10 & 5 \end{bmatrix} mod\ 26$$

$$P_2 = \begin{bmatrix} 93 & 41 \\ 90 & 45 \end{bmatrix} mod\ 26 = \begin{bmatrix} 15 & 15 \\ 12 & 19 \end{bmatrix}.$$

$$P_3 = K^{-1}.P_2\ mod\ 26$$

$$P_3 = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}.\begin{bmatrix} 15 & 15 \\ 12 & 19 \end{bmatrix} mod\ 26$$

$$P_3 = \begin{bmatrix} 111 & 167 \\ 108 & 171 \end{bmatrix} mod\ 26 = \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix}.$$

$$\therefore the\ Plain\ text = P_3 = \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix}$$

Convert the number matrix of plain text to letter matrix using Table 2:-

$$the\ Plain\ tex = \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix} = \begin{bmatrix} H & L \\ E & P \end{bmatrix}.$$
$$\therefore the\ Plain\ text = HELP$$

b. Example 2

In this case, the plain text = (I LOVE IRAQ) and the Key= [1 2 6; 0 3 5; 4 7 8]:
Constitute the plain text to square matrix (N*N), in which N=3.

$$Plain\ text = \begin{bmatrix} I & V & R \\ L & E & A \\ O & I & Q \end{bmatrix}.$$

Convert the plain text from the letter matrix to number matrix using Table 1.

$$P = \begin{bmatrix} I & V & R \\ L & E & A \\ O & I & Q \end{bmatrix} = \begin{bmatrix} 8 & 21 & 17 \\ 11 & 4 & 0 \\ 14 & 8 & 16 \end{bmatrix}$$

$$Key = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}.$$

Encryption the plain text by using (1).

$$C_1 = K.P\ mod\ 26$$

$$C_1 = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}.\begin{bmatrix} 8 & 21 & 17 \\ 11 & 4 & 0 \\ 14 & 8 & 16 \end{bmatrix} mod\ 26$$

$$C_1 = \begin{bmatrix} 326 & 230 & 118 \\ 420 & 417 & 381 \\ 557 & 608 & 580 \end{bmatrix} mod\ 26 = \begin{bmatrix} 14 & 22 & 14 \\ 4 & 1 & 17 \\ 11 & 10 & 8 \end{bmatrix}$$

$$C_2 = K.C_1\ mod\ 26$$

$$C_2 = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}.\begin{bmatrix} 14 & 22 & 14 \\ 4 & 1 & 17 \\ 11 & 10 & 8 \end{bmatrix} mod\ 26$$

$$C_2 = \begin{bmatrix} 191 & 166 & 500 \\ 356 & 402 & 534 \\ 513 & 607 & 689 \end{bmatrix} mod\ 26 = \begin{bmatrix} 9 & 10 & 6 \\ 18 & 12 & 14 \\ 19 & 9 & 13 \end{bmatrix}$$

$$C_3 = K.C_2\ mod\ 26$$

$$C_3 = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}.\begin{bmatrix} 9 & 10 & 6 \\ 18 & 12 & 14 \\ 19 & 9 & 13 \end{bmatrix} mod\ 26$$

$$C_3 = \begin{bmatrix} 505 & 357 & 385 \\ 595 & 412 & 432 \\ 771 & 539 & 553 \end{bmatrix} mod\ 26 = \begin{bmatrix} 11 & 19 & 21 \\ 23 & 22 & 16 \\ 17 & 19 & 7 \end{bmatrix}.$$

Decryption the cipher text to plain text by using key inverse and the C_3 based on (2):-

$$Key^{-1} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

$$P_1 = K^{-1}.C_3\ mod\ 26$$

$$P_1 = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} . \begin{bmatrix} 11 & 19 & 21 \\ 23 & 22 & 16 \\ 17 & 19 & 7 \end{bmatrix} mod\ 26$$

$$P_1 = \begin{bmatrix} 373 & 452 & 318 \\ 772 & 974 & 716 \\ 643 & 815 & 689 \end{bmatrix} mod\ 26 = \begin{bmatrix} 9 & 10 & 6 \\ 18 & 12 & 14 \\ 19 & 9 & 13 \end{bmatrix}.$$

$$P_2 = K^{-1}.P_1\ mod\ 26$$

$$P_2 = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} . \begin{bmatrix} 9 & 10 & 6 \\ 18 & 12 & 14 \\ 19 & 9 & 13 \end{bmatrix} mod\ 26$$

$$P_2 = \begin{bmatrix} 352 & 230 & 248 \\ 732 & 495 & 511 \\ 557 & 426 & 398 \end{bmatrix} mod\ 26 = \begin{bmatrix} 14 & 22 & 14 \\ 4 & 1 & 17 \\ 11 & 10 & 8 \end{bmatrix}.$$

$$P_3 = K^{-1}.P_2\ mod\ 26$$

$$P_3 = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} . \begin{bmatrix} 14 & 22 & 14 \\ 4 & 1 & 17 \\ 11 & 10 & 8 \end{bmatrix} mod\ 26$$

$$P_3 = \begin{bmatrix} 242 & 281 & 277 \\ 557 & 680 & 598 \\ 430 & 554 & 562 \end{bmatrix} mod\ 26 = \begin{bmatrix} 8 & 21 & 17 \\ 11 & 4 & 0 \\ 14 & 8 & 16 \end{bmatrix} .$$

$$\therefore the\ Plain\ text = P_3 = \begin{bmatrix} 8 & 21 & 17 \\ 11 & 4 & 0 \\ 14 & 8 & 16 \end{bmatrix}$$

Convert the number matrix of plain text to letter matrix using Table 2:-

$$the\ Plain\ tex = \begin{bmatrix} 8 & 21 & 17 \\ 11 & 4 & 0 \\ 14 & 8 & 16 \end{bmatrix} = \begin{bmatrix} I & V & R \\ L & E & A \\ O & I & Q \end{bmatrix}.$$

$\therefore the\ Plain\ text$ =I LOVE IRAQ

c. Example 3

In this case, the plain text = (SOFTWARE COMPUTER) and the Key = [3 5 7 2; 1 4 7 2; 6 3 9 17; 13 5 4 16]: Constitute the plain text to square matrix (N*N), in which N=4.

$$Plain\ text = \begin{bmatrix} S & W & C & U \\ O & A & O & T \\ F & R & M & E \\ T & E & P & R \end{bmatrix}.$$

Convert the plain text from the letter matrix to number matrix using Table 1.

$$P = \begin{bmatrix} S & W & C & U \\ O & A & O & T \\ F & R & M & E \\ T & E & P & R \end{bmatrix} = \begin{bmatrix} 18 & 22 & 2 & 20 \\ 14 & 0 & 14 & 19 \\ 5 & 17 & 12 & 4 \\ 19 & 4 & 15 & 17 \end{bmatrix}$$

$$Key = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix}$$

Encryption the plain text by using (1).

$$C_1 = K.P \ mod\ 26$$

$$C_1 = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} . \begin{bmatrix} 18 & 22 & 2 & 20 \\ 14 & 0 & 14 & 19 \\ 5 & 17 & 12 & 4 \\ 19 & 4 & 15 & 17 \end{bmatrix} mod\ 26$$

$$C_1 = \begin{bmatrix} 197 & 193 & 190 & 217 \\ 147 & 149 & 172 & 158 \\ 518 & 353 & 417 & 502 \\ 628 & 418 & 384 & 643 \end{bmatrix} mod\ 26 = \begin{bmatrix} 15 & 11 & 8 & 9 \\ 17 & 19 & 16 & 2 \\ 24 & 15 & 1 & 8 \\ 4 & 2 & 20 & 19 \end{bmatrix} .$$

$$C_2 = K.C_1 \ mod\ 26$$

$$C_2 = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} . \begin{bmatrix} 15 & 11 & 8 & 9 \\ 17 & 19 & 16 & 2 \\ 24 & 15 & 1 & 8 \\ 4 & 2 & 20 & 19 \end{bmatrix} mod\ 26$$

$$C_2 = \begin{bmatrix} 306 & 237 & 151 & 131 \\ 259 & 196 & 119 & 111 \\ 425 & 292 & 445 & 455 \\ 440 & 330 & 508 & 463 \end{bmatrix} mod\ 26 = \begin{bmatrix} 20 & 3 & 21 & 1 \\ 25 & 14 & 15 & 7 \\ 9 & 6 & 3 & 13 \\ 24 & 18 & 14 & 21 \end{bmatrix}$$

$$C_3 = K.C_2 \ mod\ 26$$

$$C_3 = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} . \begin{bmatrix} 20 & 3 & 21 & 1 \\ 25 & 14 & 15 & 7 \\ 9 & 6 & 3 & 13 \\ 24 & 18 & 14 & 21 \end{bmatrix} mod\ 26$$

$$C_3 = \begin{bmatrix} 296 & 157 & 187 & 171 \\ 231 & 137 & 130 & 162 \\ 684 & 420 & 436 & 501 \\ 805 & 421 & 584 & 436 \end{bmatrix} mod\ 26 = \begin{bmatrix} 10 & 1 & 5 & 15 \\ 23 & 7 & 0 & 6 \\ 8 & 4 & 20 & 7 \\ 25 & 5 & 12 & 20 \end{bmatrix}$$

Decryption the cipher text to plain text by using key inverse and the C_3 based on (2):-

$$Key^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

$$P_1 = K^{-1}.C_3 \ mod\ 26$$

$$P_1 = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix} . \begin{bmatrix} 10 & 1 & 5 & 15 \\ 23 & 7 & 0 & 6 \\ 8 & 4 & 20 & 7 \\ 25 & 5 & 12 & 20 \end{bmatrix} mod\ 26$$

$$P_1 = \begin{bmatrix} 1008 & 237 & 255 & 651 \\ 987 & 196 & 379 & 839 \\ 737 & 214 & 471 & 507 \\ 596 & 148 & 456 & 567 \end{bmatrix} mod\ 26 = \begin{bmatrix} 20 & 3 & 21 & 1 \\ 25 & 14 & 15 & 7 \\ 9 & 6 & 3 & 13 \\ 24 & 18 & 14 & 21 \end{bmatrix} .$$

$$P_2 = K^{-1}.P_1 \ mod\ 26$$

$$P_2 = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix} . \begin{bmatrix} 20 & 3 & 21 & 1 \\ 25 & 14 & 15 & 7 \\ 9 & 6 & 3 & 13 \\ 24 & 18 & 14 & 21 \end{bmatrix} mod\ 26$$

$$P_2 = \begin{bmatrix} 1185 & 609 & 840 & 477 \\ 1213 & 591 & 926 & 548 \\ 934 & 431 & 651 & 424 \\ 862 & 314 & 696 & 331 \end{bmatrix} mod\ 26 = \begin{bmatrix} 15 & 11 & 8 & 9 \\ 17 & 19 & 16 & 2 \\ 24 & 15 & 1 & 8 \\ 4 & 2 & 20 & 19 \end{bmatrix}.$$

$$P_3 = K^{-1}.P_2\ mod\ 26$$

$$P_3 = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix} . \begin{bmatrix} 15 & 11 & 8 & 9 \\ 17 & 19 & 16 & 2 \\ 24 & 15 & 1 & 8 \\ 4 & 2 & 20 & 19 \end{bmatrix} mod\ 26$$

$$P_3 = \begin{bmatrix} 642 & 594 & 756 & 462 \\ 586 & 468 & 768 & 643 \\ 941 & 745 & 454 & 368 \\ 851 & 628 & 379 & 407 \end{bmatrix} mod\ 26 = \begin{bmatrix} 18 & 22 & 2 & 20 \\ 14 & 0 & 14 & 19 \\ 5 & 17 & 12 & 4 \\ 19 & 4 & 15 & 17 \end{bmatrix}.$$

$$\therefore the\ Plain\ text = P_3 = \begin{bmatrix} 18 & 22 & 2 & 20 \\ 14 & 0 & 14 & 19 \\ 5 & 17 & 12 & 4 \\ 19 & 4 & 15 & 17 \end{bmatrix}$$

Convert the number matrix of plain text to letter matrix using Table 2:-

$$the\ Plain\ tex = \begin{bmatrix} 18 & 22 & 2 & 20 \\ 14 & 0 & 14 & 19 \\ 5 & 17 & 12 & 4 \\ 19 & 4 & 15 & 17 \end{bmatrix} = \begin{bmatrix} S & W & C & U \\ O & A & O & T \\ F & R & M & E \\ T & E & P & R \end{bmatrix}.$$

$$\therefore the\ Plain\ text = SOFTWARE\ COMPUTER.$$

6. CONCLUSION

In this paper, we reviewed a different methods used Hill Cipher method with triple pass protocol method (TTP). The Hill Cipher Technical use a personal key in encryption and the inverse same key when used decryption. In three pass protocol any key no exchange for encryption and decryption. Apply the Hill Cipher algorithms depended on three pass protocol period (three times). We discussed security for the message sender and receiver in many cases. Finally, the result of the paper description this systems and implementation of algorithms and provides some assistance in improving encryption and decryption process to ensure network safety.

REFERENCES

[1] D. Rachmawati, M. A Budiman, L Aulya, "Three-pass protocol scheme for bitmap image security by using vernam cipher algorithm," *IOP Conferences Series: Materials Science and Engineering*, vol. 308, no. 1, 2018, Art. No. 012003, doi: 10.1088/1757-899X/308/1/012003.

[2] P. Verma and G. S. Gaba, "Coherent Caesar Cipher for Resource Constrained Devices," *International Journal of Security and Its Applications*, vol. 10, no. 5, pp. 327-336, 2016, doi: 10.14257/ijsia.2016.10.5.31.

[3] I. G. Sumarno, H. S. Tambunan, E. Irawan, H. Qurniawan and D. Hartama, "Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages," *Journal of Physics Conference Series*, vol. 1255, 2019, Art. No. 012077, doi: 10.1088/1742-6596/1255/1/012077.

[4] O. E. Omolara, A. I. Oludare, S. E. Abdulahi, "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication," *Computer Engineering and Intelligent Systems*, vol. 5, no. 5, pp. 34-46, 2014.

[5] A. Badawi, M. Zarlis, S. Suherman, "Impact three pass protocol modifications to key transmission performance," *Journal of Physics Conferences Series*, vol. 1235, 2019, Art. No. 012050, doi: 10.1088/1742-6596/1235/1/012050.

[6] A. M. H. Pardede, H. Manurung, D. Filina, "Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokume," *Journal of Teknik Informatika Kaputama (JTIK)*, vol. 1, no. 1, pp. 26-33, 2017, doi: 10.31227/osf.io/7h36y.

[7] S. Dey, "SD-AREE: A New Modified Caesar Cipher Cryptographic Method Along with Bit-Manipulation to Exclude Repetition from a Message to be encrypted," *arXiv 1205.4279v1*, pp. 1-5, 2012.

[8] S. Dey, "SD-AREE-I Cipher: Amalgamation of Bit Manipulation, Modified VERNAM CIPHER & Modified Caesar Cipher," *International Journal Modern Education and Computer Science (IJMECS)*, vol. 4, no. 6, pp. 43-49, 2012, doi: 10.5815/ijmecs.2012.06.06.

[9] T. Limbong and P. D. P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using of MATLAB," *International Journal of Engineering Research & Technology (IJERT)*, vol. 6, no. 02, pp. 175-178, 2017, doi: 10.17605/OSF.IO/PEMA5.
[10] D. Rachmawati, A. Sharif and R. Sianipar, "A combination of vigenere algorithm and one time pad algorithm in the three-pass protocol," *MATEC Web of Conferences*, vol. 197, no. 13, 2018, Art. No. 03008, doi: 10.1051/matecconf/201819703008.
[11] K. Gnana Sushma, B. V. S. S. N. Raju, "Implementation of Video Encryption using Hill Cipher in Labview," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 1S3, pp. 141-145, 2019.
[12] P. K. Dey and T. K. Dey, "Cryptographically Use Of Caesar Cipher Technique in Password Managing and Security System," *Indian Journal of Computer Science and Engineering*, vol. 6, no. 3, pp. 98-102, 2015.
[13] S. N. Gowda, "Innovative Enhancement of the Caesar Cipher Algorithm for Cryptography," *2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall)*, Bareilly, India, 2016, pp. 1-4, doi: 10.1109/ICACCAF.2016.7749010.
[14] P. Verma, G. S. Gaba and H. Monga, "Modified Caesar Cipher using Rectangular Method for Enhanced Security," *Journal of Communications Technology, Electronics and Computer Science*, no. 8, pp. 1-4, 2016, doi: 10.22385/jctecs.v8i0.116.
[15] N. Shibiraj, I. Tomba, "Modified Hill Cipher: Secure Technique using Latin Square and Magic Square," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 12, pp. 315-320, 2018, doi: 10.26438/ijcse/v6i12.315320.
[16] Z. E. Dawahdeh, S. N. Yaakob, R. R.bin Othman, "A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 349-355, 2018, doi: 10.1016/j.jksuci.2017.06.004.
[17] A. Jain, R. Dedhia and A. Patil, "Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication," *International Journal of Computer Application*, vol. 129, no. 13, pp. 6-11, 2015, doi: 10.5120/ijca2015907062.
[18] Y. Inan," Analyzing The Classic Caesar Method Cryptography," *4th International Conference on Computational Mathematics and Engineering Sciences (CMES-2019)*, vol. 23, 2019, pp. 213-220.
[19] N. N. Kucherov, M.A. Deryabin, M. G. Babenko, "Homomorphic Encryption Methods Review," *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, St. Petersburg and Moscow, Russia, 2020, pp. 370-373, doi: 10.1109/EIConRus49466.2020.9039110.
[20] N. A. Kako, "Classical Cryptography for Kurdish Language," *4th International Engineering Conference on Developments in Civil & Computer Engineering Applications*, vol. 4, 2018, pp. 20-28, doi: 10.23918/iec2018.02.
[21] A. Subandi, R. Meiyanti, C. L. M. Sandy, R. W. Sembiring, "Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification," *Journal of Advances in Science, Technology and Engineering Systems*, vol. 2, no. 5, pp. 1-5, 2017, doi: 10.25046/aj020501.
[22] B. Oktaviana and A. P. U. Siahaan, "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography," *IOSR Journal of Computer Engineering*, vol. 18, no. 4, pp. 26-29, 2016, doi: 10.9790/0661-1804032629.
[23] R. Febrianingsih and A. Hafiz, "Implementasi Kriptografi Berbasis Caesar Chiper Untuk Keamanan Data*," Journal Information of computer*, vol. 7, no. 2, pp. 81-86, 2020, doi:10.35959/jik.v7i2.163.
[24] Mesran, and S. D. Nasution, "Peningkatan Keamanan Kriptografi Caesar Cipher dengan Menerapkan Algoritma Kompresi Stout Codes," *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, vol. 4, no. 6, pp. 1209-1215, 2020, doi: 10.29207/resti.v4i6.2730.
[25] S. Abedin, T. Tasbin and A. Hira, "Optical Wireless Data Transmission with Enhanced Substitution Caesar Cipher Wheel Encryption," *2017 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Cox's Bazar, Bangladesh, 2017, pp. 552-556, doi: 10.1109/ECACE.2017.7912967.

BIOGRAPHIES OF AUTHORS

Liqaa Saadi Mezher, Master Science in Computer Engineering, B. Science in Computer and Software Engineering. She has 14 years of teaching experience. She published eight research papers at International level and two research papers al locoly. Worked at Al-Mustansiriyah University, Baghdad, Iraq.

Ayam Mohsen Abbass, Master Science in Computer Engineering, B. Science in Computer and Software Engineering. She has 14 years of teaching experience. She published many research papers at Internationally. Worked at Al-Mustansiriyah University, Baghdad, Iraq.