مجلة العلوم البحتة والتطبيقية
Journal of Pure & Applied Sciences
www.Suj.sebhau.edu.ly ISSN 2521-9200
Received 28/05/2019 Revised 21/08/2019 Published online 01/12/2019

# Three-Pass Protocol Implementation in Hill Cipher Encryption Technique

Salwa Miftah Alsharif
Faculty of Computer Science, University of Omar AL-Mukhtar,Libya
Corresponding author: salwa.alsharif@omu.edu.ly

**Abstract** Hill Cipher is a common encryption technique that relies on Algebra of matrices in the selecting of the encryption key, which is expected to complicate the various techniques of crypt-analyst. But it has a disadvantage which exchange the keys between recipients, the receiver can't decrypt cipher text until the sender send to the receiver the key used to encryption the data. So that, he can restore the cipher text into plain text. Therefore, the message will be subjected to the exposing plain text and decrypt the cipher text. Three-Pass Protocol is protocol that allows both senders and receivers to communicate without the key exchange.The main goal in the research is to strengthen the security of the data, used in combination Hill Cipher algorithm for encryption and decryption while Three-Pass Protocol used to send process.The technique of Three-Pass Protocol is applied in the Hill Cipher and the results have been analyzed.The result of the analysis indicated that the encryption has been enhanced and the security improved by 85% in comparison with conventional Hill.
**Keywords:** Decryption, Encryption, Hill Cipher,Three-Pass Protocol.

# تنفيذ بروتوكول المعابر الثلاثة في تقنية تشفير هيل

سلوي مفتاح الشريف
قسم الحاسوب– كلية الآداب والعلوم– جامعة عمر المختار، ليبيا
للمراسلة: salwa.alsharif@omu.edu.ly

**الملخص** تشفير هيل هو تقنيه التشفير الشائعة التي تعتمد علي جبر المصفوفات في اختيار مفتاح التشفير، والتي من المتوقع أن تعقد التقنيات المختلفة لمحلل التشفير. ولكن لديها عيباً وهو تبادل المفاتيح بين المستلمين ، المستلم لا يمكنه فك التشفير النص المشفر حتى يرسل المرسل إليه المفتاح المستخدم لتشفير البيانات بحيث يمكنه استعادة نص المشفر إلى نص الواضح. لذلك، سيتم إخضاع الرسالة لكشف النص العادي وفك تشفير النص المشفر. بروتوكول المعابر الثلاثة هو ذلك البروتوكول الذي يسمح للمرسلين وأجهزه الاستقبال بالاتصال بدون تبادل المفاتيح، الهدف الرئيسي في البحث هو تعزيز أمن البيانات المستخدمة في الجمع بين خوارزمية تشفير هيل للتشفير وفك التشفير في حين أن بروتوكول المعابر الثلاثة يستخدم لعملية الإرسال. يتم تطبيق تقنية البروتوكولات المعابر الثلاثة في تشفير هيل وقد تم تحليل النتائج. وقد أوضحت نتيجة التحليل أن التشفير قد تم تحسينه وتحسن الأمان بنسبة 85 ٪ مقارنة مع تشفير هيل التقليدي.
**الكلمات المفتاحية:** فك التشفير، التشفير، تشفير هيل، بروتوكول المعابر الثلاث.

## 1. Introduction

The Hill's matrix algorithm is known for being the first purely Algebraic cryptography system and for starting the entire field of algebra cryptology [1][ 2], Hill cipher has several advantages, such as disguising letter frequencies of the plain text, its simplicity because of using matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput. However, the drawback of this algorithm is that the inverse of the matrix used for encrypting the plain text does not always exist. So, if the matrix is not invertible, the encrypted text cannot be decrypted. Moreover, the exchange of keys between senders and receivers ,the receiver can't decrypt cipher text until the sender send to the receiver the key used to encryption the data so that he can restore the cipher text into plain text . Hill Cipher can be easily broken with a known plaintext attack revealing weak security [3][4]. This is the problem of Hill Cipher. Hill Cipher is very difficult to solve if cryptologist has only the cipher text, but it can be solved easily if the cryptologist has a part of the plaintext Both participants must generate a key matrix to encrypt the message [4] [5], the inverse key will be applied to the encrypted text when the decrypted occurs. Since we use the key as a password to encrypted and decrypted the message, the key must be sent or give to someone who is responsible for decrypting the message. The key must be distributed, and that 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. There several changes of Hill Cipher part to make Both Algorithms work together.

In the application of Three-Pass Protocol in Hill Cipher, the plain text cannot directly transform to cipher text and then encrypt the cipher text one more time . If we do this when doing the decryption, the plain text 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 2x2 the plain text block will be 2x2is totally different from the usual Hill Cipher encryption that uses different matrix order [4].

Three-PassProtocols is a password-based key exchange model that is widely used to allow one party to send messages securely to a second party without having to exchange or distribute encryption keys. It is called a Three-Pass Protocol for the exchange three times to authenticate the sender and recipient of the first protocol. This protocol may be realized by using exclusive-OR (XOR) operations [6]. It is developed by Adi Shamir developed around 1980, the basic concept of the Three-Pass Protocol is that each party has the encryption key , a private key or a private decryption. Both sides independ-ently using the key to encrypt messages first, and then to decrypt the message. This protocol works in commutative ciphers or LIFO method. Commutative means that the order of encryption and decryption is interchangeable(Encryption A-Encryption B-Decryp-tion A - Decryption B) [7].

**2. Related Work**

Considered Three-Pass Protocol is an active area of research. A number of techniques implemented on Three-Pass Protocol . Robbi rahim , Ali ikhwan [8], they was able to the recognition of the weakness in Three-Pass Protocol when using when using XOR function can be learned for the original message kripanalis expert or also randomly tests using other functions. The downside of Three-Pass Protocol does not mean that cannot be resolved, one way to cope with combining or replacing the XOR function in the process of Three-Pass Protocol, basically three pass protocol does not depend on the XOR function so that it can be replaced by other algorithms such as algorithms One Time Pad, Vigenere cipher, RSA, PohligHellman, McAlice, Triple DES, RC4 and many other algorithms that can be implemented into Three- Passes Protocol.

They proposed Boni oktaviana, Andysah putera siahaan [9], combining classical cryptography the Caesar Cipher and Three-Pass Protocol, the division of encryption to into two parts, classic and modern cryptography , the oldest classical cryptography is the Caesar cipher, where the Caesar cipher algorithm that is by changing the position of the initial letter of the alphabet or also called ROT algorithm. Three-PassesProtocol is a modern method cryptography. The basic concept of the Three-Pass Protocol is that each party has a private encryption key and a private decryption key . The sender does not have to share a key to the receiver, the main goal in the research is to strengthen the security of the data is used in combination Caesar cipher algorithm for encryption and decryption while Three-Pass Protocol used to send process. The benefits of this research are that we can send messages without sharing encryption keys with other parties and strengthen Caesar Cipher algorithm in the process of sending messages. They proposed Darsono nababan and Robbi rahim[10] , combination Secret Sharing Protocol and Three-Pass Protocol algorithm implementation on Three-Pass Protocol better than the invitation XOR logic (Three-Pass) because it is already applying a matter of mathematical computation is quite compl-ex, making it difficult to obtain the plaintext crypta-nalysis especially by applying other algorithms such as PohligHellman, DES, 3DES and AES even apply-ing modern mathematics as a basis for calculateeon, an increasingly sophisticated mathematical calcula-teions ciphertext increasingly difficult to penetrate such as RSA and AES requiring billion years based on research. The findings in this research include the combination of protocols Secret Sharing, and Three-Pass managed to secure messages and send these messages to each recipient and managed to secure shares.

In this study, they proposed Agung purnomo sidik , Syahril efendi, et.al, [11], the technique used to cover the weakness of one-time pad algorithm is by changing each ciphertext generated from the three paths in the Three-PassesProtocol scheme. Cipher text modification is performed by encrypting the cipher text by using the RSA and Elgamal algorithms to generate super ciphertext. The first line and the third line are encrypted by using the RSA algorithm and the second line is using ElGamal algorithm. Both algorithms are aimed at keeping no secret key exchange which is a major requirement of the Three- Passes Protocol scheme. The evaluation results show that the weakness of one-time pad algorithm can be overcome. Although the processing time of three pass protocol increases, but the longer the plaintext character the closer the processing time ratio to one. The research shows The only way for plaintext to be formed by cryptoanalysis is they must succeed to decrypt the three super ciphertexts back into the three initial ciphertexts first.

They proposed Abdurrahman Ridho, et.al, [12], whether the Affine Cipher Algorithm with One Time Pad Cipher using the Three-Pass Protocol method can be used to encrypt and decryption the text message. But the conclusions that can be drawn from this research are: Affine Cipher and One Time Pad Cipher algorithms cannot be combined in the Three Pass Protocol Method .Not all Ciphers can be combined in the Three- Passes Protocol Method .And Affine Cipher algorithm can encrypt well .The One Time Pad Cipher algorithm can encrypt well .Affine Cipher's algorithm cannot decrypt the results of the One Time Pad Cipher's decryption

Proposed Robbi rahim[13], the implementation of Pohlig-hellman algorithm to the Three-Pass Protocol can be done well, the use of algorithms such as Euler totient, GCD, Rabin Miller, Extended Euclidean in the encryption process and decryption Pohlig-hellman algorithm can improve security especially from the key side used. The development of the Pohlig-helman algorithm is particularly possible at the time encryption and decryption combined with other algorithms or also the Three-Pass Protocol can be upgraded by combining with other protocols such as secret sharing or blind signatures.

A .P .U . Siahaan [5], has also used the concept of Three-PassProtocol in Hill Cipher, howe-ver this work did not analyze the result to improve the effectiveness of this method. Therefore, in this work we have implemented the Three-Pass Protocol in Hill Cipher technique and the results have been analyzed. The result of the analysis indicated that

the encryption has been enhanced and the security improved by 85% in comparison with conventional Hill.

**3. METHODOLOGY**

This study will be modified the encryption block with a square block. Which means there will swap the values of a column and the excepting row for the main diameter values of the cipher text. Encryption will be done twice in a row by both the sender and receiver of the message and using inverse cipher text in Hill Cipher algorithm, as well as the decryption process performed twice in succession by the receiver and sender of the message. It is processed through the encryption and decryption process. There are three stages in the process of encryption and decryption of the message. Three-Pass Protocol process on the sender and receiver use each key and requires no key exchange , this study are aimed at keeping no secret key exchange which is a major requirement of the Three-Pass Protocol. The plain text used in this study consisted of upper-case and lower-case letters, numbers 0 through 9 and two particular characters such as space and period. In this combination process that using a Hill cipher algorithm to perform encryption and decryption of messages been sent, while for the message delivery process using Three-Pass Protocol. In Figure (1) is an explaining to the user interface, a process key generation, encryption, and decryption process in a simulation program.

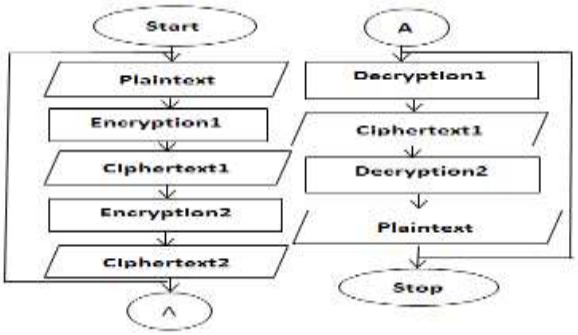


**Fig. 1**: Three-Pass Protocol flow chart

Hill Cipher is the language of the dependent encryption method. That's why plain text all charact-ers will be in lower-case, and we'll remove the blank characters as well. Then, every letter will be replaced by its index value in the alphabet, each plain text letters is assigned a numerical value like a =0,b=1,c=2,d=3,... .....z= 25.

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

**Fig. 2**: 26 character alphabet table

**Selecting a Key**: Both parties sender and receiver need to agree with a secret key. This key should be a square matrix. The key matrix could have an inverse matrix. This means, determinant of the matrix must not be 0.

**Matrix size**: Encryption will be handled by multiplying message and key. This requires that column size of the message must be equal to row size of the key.

**Encryption:** The basic theory is the multiplication between the matrix and the inverse of the matrix. Multiplication might produce values greater than the alphabet size. That's why, we will apply modular arithmetic. Here is, 26 refers to the size of English alphabet. We can consume either mutual or dot functions.

Hill encryption can be performed by computing :

$C = K_{21}\ k_{22}\ p_2 \quad C=E_K(P) = (K*P) \bmod 26.$

$$\begin{pmatrix} k_{11} & k_{12} \\ k21 & k22 \end{pmatrix} * \begin{pmatrix} p_1 & p_3 \\ p2 & p4 \end{pmatrix} \quad \text{mod total character.....1}$$

**Inverse Key:** Multiplying cipher text and inverse of key will create plain text. Here, we need to find the inverse of key. Finding matrix inverse is a complex operation. Even though, jumpy has a matrix inverse function. On the other hand, Sym-Py handles modular arithmetic for matrix inverse operations easily. We can validate inverse key matrix.

Multiplication of key and inverse key must be equal to identity matrix.

**Decryption:** Multiplying the inverse key and cipher text will create plaintext.

$P=D_{K^{-1}}(C) = (K^{-1} * C) \bmod 26.$

$$P= \begin{pmatrix} k_{11} & k_{12} \\ K_{21} & k_{22} \end{pmatrix} * \begin{pmatrix} c_1 & c_3 \\ c_2 & c_4 \end{pmatrix} \text{mod total character.....2}$$

**4. Experiment and Testing**

In this section, we try to prove the technique. Let's take an example below : Plain text : HELP.

**Plain text :** HELP $\begin{pmatrix} 7 & 11 \\ 4 & 15 \end{pmatrix}$.....(1)

$Key_1 = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix}$, $key_2 = \begin{pmatrix} 3 & 6 \\ 4 & 9 \end{pmatrix}$

**Inverse key :** Now we prove that the keys provided are invertible.

$Key_1 = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix}$

Determinant : (3 * 5 - 2 * 3 )mod 26 = 9

(D ≠ 0 and D ≠ Even).

$9 * 1/9 = 1 \bmod 26$

$$\begin{pmatrix} 5 & -2 \\ -3 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \bmod 26$$

$$= 3* \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \bmod 26 = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$$

Then $k_1^{-1} = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$ .....(2)

$key_2 = \begin{pmatrix} 3 & 6 \\ 4 & 9 \end{pmatrix}$

Determinant : (3 * 9 - 6 * 4 )mod 26 = 3

(D ≠ 0 and D ≠ Even).

$3 * 1/3 = 1 \bmod 26$

$$\begin{pmatrix} 3 & -6 \\ -4 & 9 \end{pmatrix} = \begin{pmatrix} 3 & 20 \\ 22 & 9 \end{pmatrix} \bmod 26$$

$$= 9* \begin{pmatrix} 9 & 20 \\ 22 & 3 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 & 24 \\ 16 & 1 \end{pmatrix}$$

Then $k_2^{-1} = \begin{pmatrix} 3 & 24 \\ 16 & 1 \end{pmatrix}$ .....(3)

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

**Encryption 1 :**

Plain text : HELP $\begin{pmatrix} 7 & 11 \\ 4 & 15 \end{pmatrix}$

Cipher text$_1$ = $\begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix} * \begin{pmatrix} 7 & 11 \\ 4 & 15 \end{pmatrix}$ mod 26.

$C_1$ = (3*7+2*4) mod 26
= 3 mod 26 = 3.
$C_2$ = (3*7+5*4) mod 26
= 41 mod 26 =15.
$C_3$ = (3*11+2*15) mod 26
= 63 mod 26 =11.
$C_4$ = (3*11+5*15) mod 26
= 108 mod 26=4.

Cipher text$_1$ = $\begin{pmatrix} 3 & 11 \\ 15 & 4 \end{pmatrix}^T$

Cipher text$_1^T$ = $\begin{pmatrix} 3 & 15 \\ 11 & 4 \end{pmatrix}$.....(4)

**Encryption 2:**

Cipher text$_1^T$ = $\begin{pmatrix} 3 & 15 \\ 11 & 4 \end{pmatrix}$

Cipher text$_2$ = $\begin{pmatrix} 3 & 6 \\ 4 & 9 \end{pmatrix} * \begin{pmatrix} 3 & 15 \\ 11 & 4 \end{pmatrix}$ mod 26.

$C_1$ = (3*3+6*11) mod 26
= 75 mod 26 = 23.
$C_2$ = (4*3+9*11) mod 26
= 111 mod 26 =7 .
$C_3$ = (3*15+6*4) mod 26
= 69 mod 26 =17.
$C_4$ = (4*15+9*4) mod 26
= 96 mod 26=18.

= $\begin{pmatrix} 23 & 17 \\ 7 & 18 \end{pmatrix}^T$

Cipher text$_2^T$ = $\begin{pmatrix} 23 & 7 \\ 17 & 18 \end{pmatrix}$ .....(5)

Ciphertext$_2^T$ is the final result of the encryption the both methods. The decryption does the same way as earlier. The following explanation describes how it was done.

**Decryption 1**

Cipher text$_2^T$ = $\begin{pmatrix} 23 & 7 \\ 17 & 18 \end{pmatrix}$

Cipher text$_3$= $\begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix} * \begin{pmatrix} 23 & 7 \\ 17 & 18 \end{pmatrix}$ mod 26

$C_1$ = (15*23+20*17) mod 26
= 685 mod 26 = 9.
$C_2$ = (17*23+9*17) mod 26
= 544 mod 26 =24.
$C_3$ = (15*7+20*18) mod 26
= 465 mod 26 =23.
$C_4$ = (17*7+9*18) mod 26
= 281 mod 26=21.
= $\begin{pmatrix} 9 & 23 \\ 24 & 21 \end{pmatrix}^T$

Cipher text$_3^T$ = $\begin{pmatrix} 9 & 24 \\ 23 & 21 \end{pmatrix}$ .....(6)

**Decryption 2 :**

Cipher text$_3^T$ = $\begin{pmatrix} 3 & 24 \\ 16 & 1 \end{pmatrix} * \begin{pmatrix} 9 & 24 \\ 23 & 21 \end{pmatrix}$ mod 26

$P_1$ = (3*9+24*23) mod 26
= 579 mod 26 = 7.
$P_2$ = (16*9+1*23) mod 26
= 167 mod 26 =11 .
$P_3$ = (3*24+24*21) mod 26
= 576 mod 26 =4.
$P_4$ = (16*24+1*21) mod 26
= 405 mod 26=15.

Plain text = $\begin{pmatrix} 7 & 4 \\ 11 & 15 \end{pmatrix}^T$

Plain text$^T$ = $\begin{pmatrix} 7 & 11 \\ 4 & 15 \end{pmatrix}$ .....(7)

Plain text$^T$ is the final result of the decryption the both methods.

After calculation, the plain text is converted into three parts of cipher texts before finally turned back into plain text again. Each participant needs to perform two stage of calculation where the sender does the encryption and decryption. Table 1 shows the complete work of encryption and decryption processes. The sentence is “MEET ME AFTER THE TOGA PARTY”. this study are aimed at keeping no secret key exchange between sender and receiver , which is a major requirement of the three pass protocol . If someone wants to take the information, it will be suspended. In Table 1, there are three cipher texts produced. Someone might be intercepting the information. However, 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. However, in the conventional method, the key is distributed as well. It makes the key vulnerable

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

| NO | PT1 | CT1 | CT2 | CT3 | PT2 |
|---|---|---|---|---|---|
| 1 | 12 | 18 | 16 | 8 | 12 |
| 2 | 4 | 24 | 4 | 6 | 4 |
| 3 | 4 | 4 | 2 | 22 | 4 |
| 4 | 19 | 3 | 7 | 5 | 19 |
| 5 | 12 | 18 | 10 | 10 | 12 |
| 6 | 4 | 10 | 6 | 22 | 4 |
| 7 | 0 | 4 | 6 | 16 | 0 |
| 8 | 5 | 25 | 7 | 9 | 5 |
| 9 | 19 | 13 | 1 | 3 | 19 |
| 10 | 4 | 11 | 15 | 21 | 4 |
| 11 | 17 | 25 | 21 | 22 | 17 |
| 12 | 19 | 16 | 10 | 5 | 19 |
| 13 | 7 | 3 | 25 | 5 | 7 |
| 14 | 4 | 7 | 1 | 17 | 4 |
| 15 | 19 | 15 | 23 | 18 | 19 |
| 16 | 14 | 23 | 7 | 12 | 14 |
| 17 | 6 | 18 | 12 | 4 | 6 |
| 18 | 0 | 19 | 12 | 3 | 0 |
| 19 | 15 | 18 | 9 | 0 | 15 |
| 20 | 0 | 19 | 9 | 0 | 0 |
| 21 | 17 | 11 | 25 | 13 | 17 |
| 22 | 19 | 16 | 4 | 24 | 19 |
| 23 | 24 | 16 | 6 | 19 | 24 |

**5. Evaluation and Results**

The evaluating performance of encryption technique to enhance the security were conducted using Three-Pass Protocol processes in Hill cipher. Figure (2) shows the relationship between plain text against of cipher text (PT,CT1), and the ratio extent of spacing and the difference between plain-text against of cipher text = 43%.

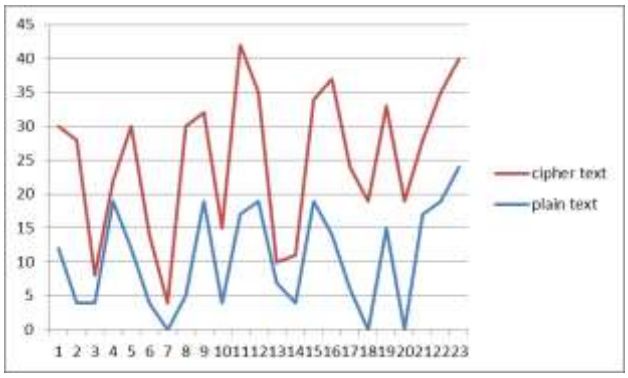


**Fig. 3:** Shows ratio of spacing CT1.

Figure (4) shows the percentage of spacing of plain text letters against of cipher text ,that show performance one stage of the encryption process. For example when m=12 is one of the letter of the plain text , be the same letter is encrypted in cipher text s=18.

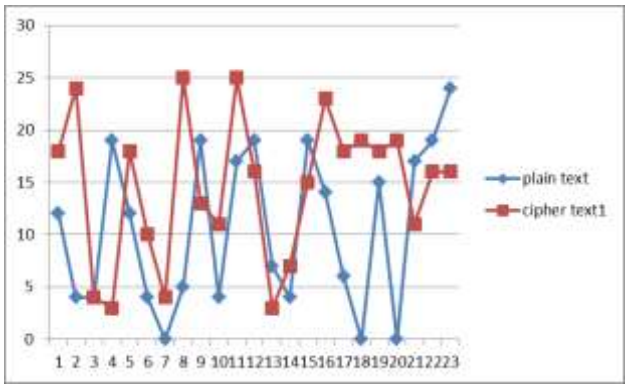


**Fig. 4**: Shows results the plain text of CT1 processe.

Figure (5) shows results the superiority of cipher text2 over cipher text1 in terms of strength secret message . It shows also that best performance two stage of the encryption , plain text is turned into two parts of cipher text before finally turned back into plaintext again .The cipher text is more steeper beyond plain text range, this means as the more encryption the greater the more of the security more. The performance results two stage the encryption is CT1=43% , CT2=65%.

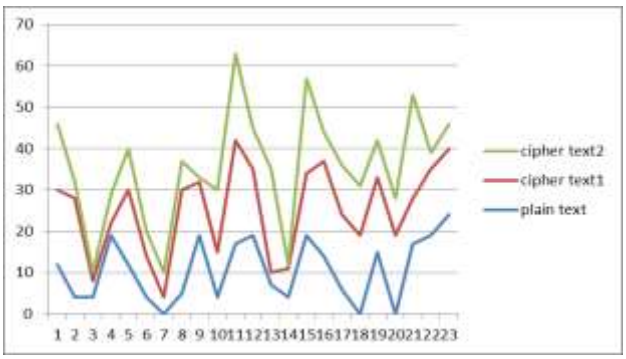


**Fig. 5**: Shows Best performance results Three-Pass Protocol implementation in two stage encryption.

Figure (6): shows results the superiority of cipher text3 over cipher text2 and cipher text1 in terms of strength secret message . It shows also that best performance three stage of the encryption and the relationship between the best performance results Three-Pass Protocol processes in Hill cipher the more encryption the greater the secret more .The Three-Pass Protocol implementation in Hill cipher is significantly higher than that of the traditional Hill cipher. The reason that to keep both not exchange keys between the sender and the recipient each is using its own key for the message encryption and decryption process.Best performance results Three-Pass Protocol processes is CT1=43%, CT2=65%, CT3 =85%.

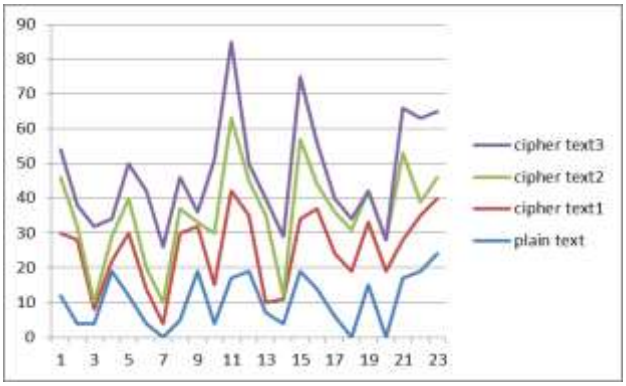


**Fig. 6**: Shows Best performance results Three-Pass Protocol implementation in Hill cipher.

Figure (7): shows ratio into best performance results Three-Pass Protocol processes in Hill cipher encrypt-tion when the plain text is variables(0-24)and CT1=43%,CT2=65%,CT3 =85%. Which demonstrates much better Three-Pass Protocol performance than conventional Hill cipher . In summary, the overall performance of combination between Three-Pass Protocol in Hill cipher is very high. It has a strong ability to more secure and confidential.

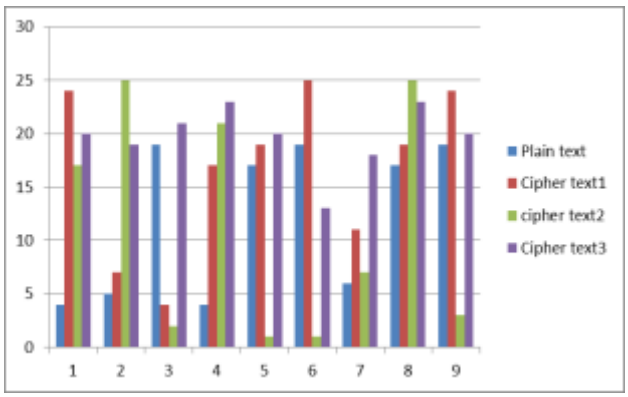


**Fig. 7**:The best performance results Three-Pass Protocol in Hill cipher.

**6. Conclusion**

Conclude that Three-Pass Protocol can be applied in Hill Cipher encryption. The result of the analysis indicated that the encryption has been enhanced and the security improved by 85% in comparison with conventional Hill. Three-PassProtocol is the best technique to gain the cipher text resulted is guaranteed and secret more. The process of sending secret message is no longer need to share a key to the sender of the message when the application of Three-Pass Protocol in Hill Cipher, Percentage of obtained from performing results Three-PassProtocol processes in Hill Cipher is CT1=43%, CT2=65%,CT3 =85% much better than conventional Hill Ciphe ,the process of sending the message will be more secure and confidential by combining Three-Pass Protocol and Hill Cipher.

**References**

[1]- Chase, J., & Davis, M, “Extending the Hill Cipher,” 2010.

[2]- Khalaf, A. A., El-Karim, M. S. A., & Hamed, H. F. “A Triple Hill Cipher Algorithm Proposed to Increase the Security of Encrypted Binary Data and its Implementation Using FPGA", 2016 18th Internatio-nal Conference on Advance Communication Techno-logy (ICACT). IEEE, 2016.

[3]- Saeednia, S., "How to make the Hill cipher secure." Cryptologia 24.4 (2000): 353-360.

[4]- Rahman, M. N. A., Abidin, A. F. A., Yusof, M. K., & Usop, N. S. M. Usop, "Cryptography: a new approach of classical Hill cipher." International Journal of Security and Its Applications 7.2 (2013): 179-190.

[5]- Siahaan, A. P. U.,"Three-Pass Protocol Concept in Hill Cipher Encryption Technique." International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2017).

[6]- Kanamori, Y., & Yoo, S. M. ,"Quantum three-pass protocol: key distribution using quantum superposition states." arXiv preprint arXiv:1004.0599 (2010) .

[7]- Rahim, R., & Ikhwan, A., "Study of Three Pass Protocol on Data Security." International Journal of Science and Research (IJSR) 5.11 (2016): 102-104.

[8]- Rahim, R., & Ikhwan, A.,"Study of Three Pass Protocol on Data Security." International Journal of Science and Research (IJSR) 5.11 (2016): 102-104.

[9]- Oktaviana, B., & Siahaan, A. P. U., "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography." IOSR Journal of Computer Engineering 18.4 (2016): 26-29.

[10]- Nababan, D., & Rahim, R. ,"Security Analysis Combination Secret Sharing Protocol and Three-Pass Protocol." Journal of Physics: Conference Series. Vol. 1175. No. 1. IOP Publishing, 2019.

[11]- Sidik, A. P., Efendi, S., & Suherman, S., "Improving One-Time Pad Algorithm on Shamir’s Three-Pass Protocol Scheme by Using RSA and ElGamal Algorithms." Journal of Physics: Conference Series. Vol. 1235. No. 1. IOP Publishing, 2019.

[12]- Ridho, A., Dewi, A. M., Siregar, R., Zarlis, M., & Hartama, D. ,"Analysis of Possibility of the Combination of Affine Cipher Algorithm with One Time Pad Cipher Using the Three-Pass Protocol Method in Text Security." Journal of Physics: Conference Series. Vol. 1255. No. 1. IOP Publishing, 2019.

[13]- Rahim, R., "Applied Pohlig-Hellman algorithm in three-pass protocol communication." Journal of Applied Engineering Science 16.3 (2018): 424-429.