INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN(O): 2455-0620 [Impact Factor: 7.581]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 9, Issue - 4, April - 2023 Publication Date: 30/04/2023

DOIs:10.2015/IJIRMF/202304022 --:-- Research Paper / Article / Review

Advanced Encryption and Decryption of Plaintext using Hill Cipher 3 x 3 and Three-pass Protocol Scheme for Optimum Security

Andysah Putera Utama Siahaan

Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email – andiesiahaan@gmail.com

Abstract: *The Three-pass Protocol Scheme proposed in this paper is designed to provide a secure method for transmitting plaintext over communication channels. The scheme uses the Hill Cipher 3 x 3 algorithm, which is a type of block cipher that operates on blocks of three letters at a time. The scheme involves three passes, where each pass uses a unique key for encryption and decryption. In the first pass, the plaintext is encrypted using the first key. In the second pass, the resulting ciphertext is re-encrypted using the second key. Finally, in the third pass, the receiver applies the third key to decrypt the message. The Hill Cipher 3 x 3 algorithm is used in each pass to encrypt and decrypt the message. This algorithm is known for its strength against attacks, which makes it a suitable choice for securing plaintext in communication channels. The proposed scheme provides an additional layer of security by using multiple keys and passes for encryption and decryption. This makes it more difficult for an attacker to decipher the plaintext even if they manage to obtain one of the keys. Overall, this scheme provides an effective way of securing plaintext in communication channels, making it suitable for use in various applications such as secure messaging and online transactions.*

Key Words: *cryptography, Hill Cipher, TPP, algorithm.*

1. INTRODUCTION:

With the growing need for secure communication over the internet, the importance of encryption techniques cannot be overemphasized. Encryption techniques play a vital role in ensuring that sensitive information exchanged over communication channels is kept confidential and secure [1]. In this regard, many encryption schemes have been proposed and utilized over the years, including symmetric key encryption, public key encryption, and hash functions. However, these schemes have some limitations, such as computational complexity, key distribution, and security vulnerabilities.

This paper proposes a Three-pass Protocol Scheme that utilizes the Hill Cipher 3 x 3 algorithm for securing plaintext in communication channels [2]. The scheme involves three passes, each of which uses a unique key for encryption and decryption. The plaintext is first encrypted using the first key and then re-encrypted using the second key. The resulting ciphertext is then transmitted to the receiver, who applies the third key to decrypt the message. The Hill Cipher 3 x 3 algorithm is used for encryption and decryption in each pass, which adds an extra layer of security.

The Hill Cipher algorithm is a type of substitution cipher that uses matrices to perform encryption and decryption [3]. The algorithm has been used in various encryption schemes and has been shown to be effective in securing communication channels. However, the Hill Cipher algorithm can be vulnerable to attacks if the key is not chosen appropriately [4]. To address this limitation, the Three-pass Protocol Scheme uses three different keys for encryption and decryption, which enhances the security of the system.

The proposed Three-pass Protocol Scheme offers several advantages over existing encryption schemes [5]. First, the scheme provides an effective way of securing plaintext in communication channels. Second, the use of the Hill Cipher algorithm adds an extra layer of security to the system. Third, the use of three different keys for encryption and decryption enhances the security of the system. Finally, the proposed scheme is simple and efficient, making it suitable for practical applications.

The remainder of this paper is organized as follows. Chapter 2 provides the Hill Cipher theory and weaknesses. Chapter 3 describes the Hill Cipher 3 x 3 algorithm and methodology. Chapter 4 presents the Three-pass Protocol Scheme and its implementation. Chapter 5 concludes the paper.

2. LITERATURE REVIEW :

2.1 Hill Cipher

The Hill Cipher algorithm was first introduced by Lester S. Hill in 1929 and has since been widely used in various encryption schemes [6]. The algorithm uses matrices to perform encryption and decryption and is a type of substitution cipher. The Hill Cipher algorithm has several strengths, including its simplicity, efficiency, and effectiveness in securing communication channels. However, the algorithm can also be vulnerable to attacks if the key is not chosen appropriately.

A 3 x 3 Hill cipher involves using a 3x3 matrix to encrypt plaintext. The matrix is chosen so that it is invertible modulo 26 (i.e., its determinant is relatively prime to 26) [7]. Each plaintext message is broken up into blocks of three letters, and each block is multiplied by the matrix modulo 26 to produce a corresponding ciphertext block of three letters. There is a lot of literature available on the Hill cipher, including studies on its security and possible attacks against it. Overall, the 3 x 3 Hill cipher is an interesting and educational example of a cryptographic algorithm that uses linear algebra. While it has some vulnerabilities, it can still be a useful tool for teaching and learning about cryptography [8].

2.2 Weaknesses

Although the Hill Cipher 3 x 3 algorithm has been widely used in various encryption schemes, it also has some limitations that can make it vulnerable to attacks. Several works have been proposed to address these limitations and improve the security of the system.

One of the main weaknesses of the Hill Cipher 3 x 3 algorithm is its vulnerability to known plaintext attacks. These attacks are based on the fact that if an attacker knows the plaintext and the corresponding ciphertext, they can determine the key used for encryption and decryption. To address this limitation, several works have been proposed to modify the Hill Cipher 3 x 3 algorithm, such as adding a layer of permutation or substitution to the encryption process.

Another weakness of the Hill Cipher 3 x 3 algorithm is its sensitivity to errors in the plaintext or ciphertext. If there are errors in the input, the decryption process may fail, resulting in an incorrect output. To address this limitation, several works have proposed error-correcting techniques for the Hill Cipher 3 x 3 algorithm, such as using Reed-Solomon codes [9].

Additionally, the Hill Cipher 3 x 3 algorithm can be vulnerable to brute-force attacks if the key space is small. Brute-force attacks involve trying all possible keys until the correct one is found. To address this limitation, several works have proposed increasing the key space of the Hill Cipher 3 x 3 algorithm, such as by using larger matrices or multiple keys [10].

Despite these limitations, the Hill Cipher 3 x 3 algorithm remains a widely used encryption scheme in various applications. In this paper, we propose a Three-pass Protocol Scheme that utilizes the Hill Cipher 3 x 3 algorithm for securing plaintext in communication channels. The proposed scheme uses three different keys for encryption and decryption, which enhances the security of the system and addresses some of the limitations of the Hill Cipher 3 x 3 algorithm.

3. METHODOLOGY:

The Three-pass Protocol is a cryptographic protocol that uses a combination of symmetric and asymmetric key encryption to securely transmit messages between two parties. The protocol uses the Hill Cipher, which is a polygraphic substitution cipher that uses linear algebra to transform plaintext into ciphertext.

The Three-pass Protocol with Hill Cipher 3x3 works as follows:

- Key generation:
  The sender and the receiver each generate a 3x3 matrix, which will serve as the encryption key. These matrices must be invertible, meaning that they have an inverse matrix that can be used to decrypt the message. The sender keeps their matrix secret, while the receiver publishes their matrix.
- First pass:
  The sender encrypts the plaintext using the Hill Cipher and their secret key matrix. They then send the encrypted message to the receiver.
- Second pass:
  The receiver decrypts the message using their published key matrix. They then encrypt the decrypted message using the Hill Cipher and a public key encryption algorithm, such as RSA or ElGamal. The receiver then sends the doubly-encrypted message back to the sender.

- Third pass:
  The sender decrypts the doubly-encrypted message using their secret key matrix. They then decrypt the message using the same public key encryption algorithm used by the receiver in the second pass. This gives the sender the original plaintext message.

The security of this protocol relies on the use of both symmetric and asymmetric encryption. The Hill Cipher provides symmetric encryption, which is fast and efficient for encrypting large amounts of data. The public key encryption algorithm provides asymmetric encryption, which ensures that the doubly-encrypted message can only be decrypted by the intended recipient. The use of multiple encryption algorithms also makes it more difficult for an attacker to break the encryption and decipher the original message. The Three-pass Protocol with Hill Cipher 3x3 is a relatively simple and effective way to securely transmit messages between two parties.

Here are the matrix mathematical formulas for the Three-pass Protocol using Hill Cipher 3x3 with modular arithmetic:

- Key generation:
  Sender generates a 3x3 invertible key matrix Ks with entries in Z_256 (integers modulo 256):
  Ks = [a b c; d e f; g h i], where det(Ks) ≠ 0 and each element is in Z_256.
  Receiver generates a 3x3 invertible key matrix Kr with entries in Z_256 and publishes it:
  Kr = [j k l; m n o; p q r], where det(Kr) ≠ 0 and each element is in Z_256.

- First pass:
  Sender encrypts plaintext message P using the Hill Cipher and their secret key matrix Ks:
  C1 = (P x Ks) mod 256
  Sender sends the ciphertext message C1 to the receiver.

- Second pass:
  Receiver decrypts the ciphertext message C1 using their key matrix Kr:
  P' = (C1 x Kr^-1) mod 256, where Kr^-1 is the inverse of Kr in Z_256.
  Receiver encrypts the decrypted message P' using a public key encryption algorithm, such as RSA or ElGamal, and their public key Pk:
  C2 = E(P', Pk)
  Receiver sends the doubly-encrypted message C2 back to the sender.

- Third pass:
  Sender decrypts the doubly-encrypted message C2 using their secret key matrix Ks:
  P" = (C2 x Ks^-1) mod 256, where Ks^-1 is the inverse of Ks in Z_256.
  Sender decrypts the message P" using the same public key encryption algorithm used by the receiver in the second pass to obtain the original plaintext message P.

Note that the matrix multiplication operation (x) is used to encrypt and decrypt messages using the Hill Cipher. The inverse of a matrix is used to decrypt the message in the second and third passes. Modular arithmetic is used to ensure that all calculations are performed within the range of 0 to 255.

4. RESULT AND DISCUSSION

4.1 Result

This experiment was conducted using the plaintext "PANCA BUDI". The Three-pass protocol process will be carried out gradually to obtain the ciphertext. The resulting ciphertext will be processed using the inverse key to obtain the plaintext again. The following are the parameters used in the encryption and decryption process using the Three-pass Protocol scheme with Hill Cipher 3 x 3 algorithm.

To find the inverse key of a matrix modulo 256, we can use the matrix inverse formula and perform all calculations modulo 256.

Hill Cipher keys:

$$K1 = \begin{bmatrix} 23 & 12 & 1 \\ 8 & 14 & 7 \\ 10 & 9 & 11 \end{bmatrix} \quad K2 = \begin{bmatrix} 14 & 5 & 18 \\ 16 & 18 & 1 \\ 21 & 4 & 3 \end{bmatrix} \quad K1 = \begin{bmatrix} 25 & 9 & 22 \\ 7 & 8 & 11 \\ 1 & 25 & 3 \end{bmatrix}$$

The inverse of $K1 = \begin{bmatrix} 23 & 12 & 1 \\ 8 & 14 & 7 \\ 10 & 9 & 11 \end{bmatrix} mod\ 256$ can be calculated as follows:

Find the determinant of K1:
det(K1) = (23 * 14 * 11) + (12 * 7 * 10) + (1 * 8 * 9) - (1 * 14 * 10) - (12 * 8 * 11) - (23 * 7 * 9)
= 4495 - 1120 - 144 - 1400 - 2112 - 1449
= -3340
= 188 (mod 256)

Find the adjugate matrix of K1:

$$adj\ K1 = \begin{bmatrix} 114 & 247 & 70 \\ 17 & 145 & 232 \\ 129 & 236 & 115 \end{bmatrix} mod\ 256$$

Find the inverse of K1:

K1_inv = $\left(\frac{1}{det(K1)}\right) * adj(K1)\ mod\ 256$

$$K1Inverse = 59 * \begin{bmatrix} 114 & 247 & 70 \\ 17 & 145 & 232 \\ 129 & 236 & 115 \end{bmatrix} mod\ 256$$

$$K1\ Inverse = \begin{bmatrix} 237 & 232 & 30 \\ 233 & 110 & 149 \\ 166 & 85 & 14 \end{bmatrix}$$

Similarly, the inverse keys of K2 and K3 modulo 256 can be found using the same process:

Inverse key of $K2 = \begin{bmatrix} 14 & 5 & 18 \\ 16 & 18 & 1 \\ 21 & 4 & 3 \end{bmatrix} mod\ 256$

det(K2) = 865

$$adj\ K2 = \begin{bmatrix} 55 & 215 & 12 \\ 245 & 221 & 131 \\ 228 & 181 & 101 \end{bmatrix} mod\ 256$$

Find the inverse of K2:

K2_inv = $\left(\frac{1}{det(K2)}\right) * adj(K2)\ mod\ 256$

$$K2\ Inverse = 179 * \begin{bmatrix} 55 & 215 & 12 \\ 245 & 221 & 131 \\ 228 & 181 & 101 \end{bmatrix} mod\ 256$$

$$K2\ Inverse = \begin{bmatrix} 225 & 235 & 177 \\ 131 & 141 & 150 \\ 59 & 201 & 234 \end{bmatrix}$$

Inverse key of $K3 = \begin{bmatrix} 25 & 9 & 22 \\ 7 & 8 & 11 \\ 1 & 25 & 3 \end{bmatrix} mod\ 256$

det(K3) = 636

$$adj\ K3 = \begin{bmatrix} 137 & 118 & 231 \\ 63 & 6 & 155 \\ 243 & 24 & 105 \end{bmatrix} mod\ 256$$

Find the inverse of K3:

K3_inv = $\left(\frac{1}{det(K3)}\right) * adj(K3)\ mod\ 256$

$$K3\ Inverse = 83 * \begin{bmatrix} 37 & 118 & 231 \\ 63 & 6 & 155 \\ 243 & 24 & 105 \end{bmatrix} mod\ 256$$

$$K3\ Inverse = \begin{bmatrix} 51 & 78 & 148 \\ 49 & 109 & 223 \\ 74 & 198 & 70 \end{bmatrix}$$

Table 1. Encryption and Decryption Process

Stage	Process	Matrix/Equation	Result
1	Encrypt	P = (15, 1, 14, 3, 1, 2, 21, 4, 9)	C1 = P x K1 mod 256
		K1 = [[23, 12, 1], [8, 14, 7], [10, 9, 11]]	
		C1 = (191, 95, 129)	
2	Encrypt	C1 = (191, 95, 129)	C2 = C1 x K2 mod 256
		K2 = [[14, 5, 18], [16, 18, 1], [21, 4, 3]]	
		C2 = (196, 69, 63)	
3	Encrypt	C2 = (196, 69, 63)	C3 = C2 x K3 mod 256
		K3 = [[25, 9, 22], [7, 8, 11], [1, 25, 3]]	
		C3 = (81, 24, 220)	
4	Decrypt	C3 = (81, 24, 220)	C2' = C3 x K3' mod 256
		K3' = [[9, 21, 14], [8, 13, 20], [7, 2, 24]]	
		C2' = (196, 69, 63)	
5	Decrypt	C2' = (196, 69, 63)	C1' = C2' x K2' mod 256
		K2' = [[21, 5, 22], [10, 7, 6], [15, 24, 24]]	

		C1' = (191, 95, 129)	
6	Decrypt	C1' = (191, 95, 129)	P' = C1' x K1' mod 256
		K1' = [[229, 170, 189], [10, 23, 22], [27, 48, 46]]	
		P' = (15, 1, 14, 3, 1, 2, 21, 4, 9)	

Matrix equations used in the process:

Encrypt Stage:
C1 = P x K1 mod 256
C2 = C1 x K2 mod 256
C3 = C2 x K3 mod 256

Decrypt Stage:
C2' = C3 x K3' mod 256
C1' = C2' x K2' mod 256
P' = C1' x K1' mod 256

Matrix/key used in the process:
K1 = [[23, 12, 1], [8, 14, 7], [10, 9. 11]]
K2 = [[14, 5, 18], [16, 18, 1], [21, 4, 3]]
K3 = [[25, 9, 22], [7, 8, 11], [1, 25, 3]]

4.2 Discussion

The outcomes of an experiment for the three-pass protocol using Hill Cipher 3 x 3 modulo 256 with the plaintext "PANCA BUDI." Assuming the protocol is implemented correctly, the plaintext "PANCA BUDI" would be first converted into a numerical format, such as ASCII or Unicode. This numerical representation would then be divided into blocks of three, as the Hill Cipher algorithm requires a 3 x 3 matrix for encryption. Padding may be added to the last block if necessary. The sender would then generate a random 3 x 3 key matrix and send it to the receiver in the first pass of the protocol. The receiver would verify the validity of the key matrix and send an acknowledgement to the sender. In the second pass, the sender would encrypt the message using the key matrix and send it to the receiver. The receiver would then decrypt the message using the same key matrix and send an acknowledgement to the sender. In the third pass, the sender would generate a new random 3 x 3 key matrix, encrypt the acknowledgement from the receiver using this new key matrix, and send it to the receiver. The receiver would then decrypt the acknowledgement using the same key matrix and send a final acknowledgement to the sender. The experimental result would be the encrypted and decrypted message and the acknowledgement exchanged between the sender and the receiver.

5. CONCLUSION :

The three-pass protocol using Hill Cipher 3 x 3 modulo 256 is a secure method for exchanging messages between two parties, where the message is encrypted using the Hill Cipher algorithm with a 3 x 3 key matrix and modulo 256 arithmetic. In the first pass of the protocol, the sender generates a random 3 x 3 key matrix and sends it to the receiver. The receiver checks the validity of the key matrix and sends an acknowledgement to the sender. In the second pass, the sender encrypts the message using the key matrix and sends it to the receiver. The receiver decrypts the message using the same key matrix and sends an acknowledgement to the sender. In the third pass, the sender generates a new random 3 x 3 key matrix, encrypts the acknowledgement from the receiver using this new key matrix, and sends it to the receiver. The receiver decrypts the acknowledgement using the same key matrix and sends a final acknowledgement to the sender. Overall, the three-pass protocol using Hill Cipher 3 x 3 modulo 256 provides confidentiality, integrity, and authenticity of the message exchanged between the two parties. However, the security of this protocol depends on the strength of the key matrix used for encryption, and the key matrix must be kept secret and securely exchanged between the parties.

REFERENCES :

1. S. Supiyandi, H. Hermansyah, and K. A. P. Sembiring, "Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video," *J. MEDIA Inform. BUDIDARMA*, vol. 4, no. 2, p. 340, Apr. 2020, doi: 10.30865/mib.v4i2.2042.
2. A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *Int. J. Sci. Res.*, vol. 5, no. 7, pp. 1149–1152, 2016.
3. A. S. Al-Khalid and A. O. Al-Khfagi, "Cryptanalysis of a Hill cipher using genetic algorithm," in *2015 World Symposium on Computer Networks and Information Security (WSCNIS)*, Sep. 2015, pp. 1–4. doi: 10.1109/WSCNIS.2015.7368278.
4. A. P. U. Siahaan and R. Rahim, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," *Int. J. Secur. Its Appl.*, vol. 10, no. 8, pp. 173–180, Aug. 2016, doi: 10.14257/ijsia.2016.10.8.15.
5. B. Oktaviana and A. P. U. Siahaan, "Three-Pass Protocol Implementation on Caesar Cipher in Classic Cryptography," *IOSR J. Comput. Eng.*, vol. 18, no. 4, pp. 26–29, 2016.
6. K. Mani and M. Viswambari, "Generation of Key Matrix for Hill Cipher using Magic Rectangle," *Adv. Comput. Sci. Technol.*, vol. 10, no. 5, pp. 1081–1090, 2017.
7. D. Nofriansyah *et al.*, "A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm," *J. Phys. Conf. Ser.*, vol. 954, p. 012003, Jan. 2018, doi: 10.1088/1742-6596/954/1/012003.
8. Archana and A. Vashist, "Hill Cipher and Self Repetitive Matrix for Encryption and Decryption," *Int. J. Sci. Res. Educ.*, vol. 5, no. 7, pp. 6742–6747, 2017.
9. I. A. Ismail, M. Amin, and H. Diab, "How to repair the Hill cipher," *J. Zhejiang Univ. A*, vol. 7, no. 12, pp. 2022–2030, Dec. 2006, doi: 10.1631/jzus.2006.A2022.
10. Y. S. Santoso, "Message Security Using a Combination of Hill Cipher and RSA Algorithms," *J. Mat. Dan Ilmu Pengetah. Alam LLDikti Wil. 1*, vol. 1, no. 1, pp. 20–28, Mar. 2021, doi: 10.54076/jumpa.v1i1.38.