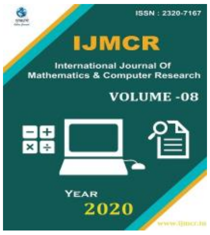
International Journal of Mathematics and Computer Research
ISSN: 2320-7167

Volume 11 Issue 06 June 2023, Page no. – 3503-3505

Index Copernicus ICV: 57.55, Impact Factor: 7.362

DOI: 10.47191/ijmcr/v11i6.06



A Novel Approach in Hill Cipher Cryptography

G. Rekha[1], V. Srinivas[2]
[1]Department of Humanities and Sciences, Malla Reddy College of Engineering and Technology.
[2]Department of Mathematics, Osmania university.

ARTICLE INFO

Published online:
29 June 2023

Corresponding Author:
G. Rekha

ABSTRACT

Cryptography plays a vital role in securing sensitive information in various domains. Hill cipher, a classic encryption technique, has been widely used for its simplicity and effectiveness. However, the original Hill cipher is susceptible to certain attacks due to its limited key space and vulnerable characteristics. In this study, we propose an enhanced version of the Hill cipher called the “Block Hill Cipher” that overcomes the limitations of the original algorithm while preserving its fundamental principles. To increase the safety and effectiveness of the encryption process, the Block Hill Cipher offers a number of unique ideas. The Block Hill Cipher encrypts blocks of characters rather than single4 characters, making it possible to encrypt longer sequences at once. By expanding the key space and making the cipher more resistant to statistical attacks, this method greatly enhances the cipher’s overall security. In light drawbacks the present paper deals with a fresh strategy in which our algorithm by incorporating while upholding the Hill cipher’s fundamental ideas. Hence on the findings of the study may be useful cryptographic tool ranging from communication systems to data storage and transmission in modern digital environments.

KEYWORDS: Cryptography, Symmetric Cryptography, Hill Cipher, Encryption and Decryption.

1. INTRODUCTION

The science or art of enclosing the methods and principles of transforming a message from plaintext, which is easily understood, into cipher text, which makes no sense, and then returning the message to plaintext, which is easily understood, is known as cryptography. In the modern day, cryptography is regarded as a part of both computer science and mathematics and is closely related to information theory, engineering, and computer security. Yet , in the distant past, the term "cryptography" exclusively applied to the encryption and decryption of messages using private keys. Asymmetric and symmetric cryptography are now the two main classifications used to describe encryption. The transmitter and receiver utilize the same key for encryption and decryption in symmetric cryptography, whereas two distinct keys are used in asymmetric cryptography. If the process of encryption and decryption uses block of characters then it is called Block Cipher. The process of converting the plaintext into unintelligible form is called Encryption[2] and the process of converting the encrypted message to get back plaintext is called Decryption [2].

In the Hill Cipher, the plaintext is transformed into integers and organized into matrices. A non-singular matrix A is used as the encryption key, and encryption is carried out using the formula C = A B(mod26), where B is the matrix of the plaintext and C is the matrix of the encrypted message. Using B = A^{-1}C (mod26), the receiver receives the matrix of the plaintext B after getting the matrix C. The Hill Cipher has a flaw in that the key A can be easily figured out if an attacker has access to the matrices C and B. A change to the Hill Cipher was suggested by the authors in [1].

We now propose and present a novel method which uses two keys and is secured against known plaintext attacks.

2. PROPOSED ALGORITHM

Step 1: Assign
A→1, B→2 , C→3…..Y→25 , Z→26 and Space as 27.
Step 2: Let n be any natural number greater than 1.
Step 3: Convert the message into blocks and form square matrices of order n . If the last block falls short of characters then filling can be done using empty spaces.
Step 4: Let P and Q be two keys which are square matrices of order n where Q is non-singular .
Step 5: If A is the matrix of the plaintext then the matrix B of Ciphertext is given by $B = (A + P)Q,$ which is Encryption .
Step 6: The matrix of plaintext A is obtained using $BQ^{-1} - P$, which is Decryption .

To see how the above algorithm works let us discuss the illustrations.

ILLUSTRATION 1:

Let n = 3 then each block contain n^2 = 9 characters.

Let the plaintext be

“THINK POSITIVE BE POSITIVE”.

Converting the message into blocks , we get three blocks containing 27 characters of each.

“THINK#POS” , “ITIVE#BE#” , “POSITIVE#” where ‘#’ stands for space and padding is also done for the empty spaces.

Converting to numbers and forming square matrix of order 3 , we get the matrices of plaintext as

$$A_1 = \begin{bmatrix} 20 & 8 & 9 \\ 14 & 11 & 27 \\ 16 & 15 & 19 \end{bmatrix} ,$$

$$A_2 = \begin{bmatrix} 9 & 20 & 9 \\ 22 & 5 & 27 \\ 2 & 5 & 27 \end{bmatrix} , A_3 = \begin{bmatrix} 16 & 15 & 19 \\ 9 & 20 & 9 \\ 22 & 5 & 27 \end{bmatrix}$$

Let $P = \begin{bmatrix} 1 & 0 & -2 \\ 2 & 3 & -4 \\ 3 & 3 & -6 \end{bmatrix}$ and $Q = \begin{bmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{bmatrix}$ be the keys where Q is a non-singular matrix

$$B_1 = \left(\begin{bmatrix} 20 & 8 & 9 \\ 14 & 11 & 27 \\ 16 & 15 & 19 \end{bmatrix} + \begin{bmatrix} 1 & 0 & -2 \\ 2 & 3 & -4 \\ 3 & 3 & -6 \end{bmatrix} \right) Q$$

$$B_1 = \begin{bmatrix} 21 & 8 & 7 \\ 16 & 14 & 23 \\ 19 & 18 & 13 \end{bmatrix} \begin{bmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 79 & -94 & 123 \\ 76 & -113 & 143 \\ 93 & -124 & 161 \end{bmatrix}.$$

$$B_2 = \left(\begin{bmatrix} 9 & 20 & 9 \\ 22 & 5 & 27 \\ 2 & 5 & 27 \end{bmatrix} + \begin{bmatrix} 1 & 0 & -2 \\ 2 & 3 & -4 \\ 3 & 3 & -6 \end{bmatrix} \right) Q$$

$$B_2 = \begin{bmatrix} 10 & 20 & 7 \\ 24 & 8 & 23 \\ 5 & 8 & 21 \end{bmatrix} \begin{bmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{bmatrix}$$

$$B_2 = \begin{bmatrix} 70 & -97 & 127 \\ 88 & -119 & 151 \\ 31 & -60 & 73 \end{bmatrix}.$$

$$B_3 = \left(\begin{bmatrix} 16 & 15 & 19 \\ 9 & 20 & 9 \\ 22 & 5 & 27 \end{bmatrix} + \begin{bmatrix} 1 & 0 & -2 \\ 2 & 3 & -4 \\ 3 & 3 & -6 \end{bmatrix} \right) Q$$

$$B_3 = \begin{bmatrix} 17 & 15 & 17 \\ 11 & 23 & 5 \\ 25 & 8 & 21 \end{bmatrix} \begin{bmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{bmatrix}$$

$$B_3 = \begin{bmatrix} 81 & -113 & 145 \\ 79 & -107 & 141 \\ 91 & -120 & 153 \end{bmatrix}.$$

Decryption

The matrices of the plaintext A_1 ,A_2 and A_3 are obtained by using $A_1 = (B_1 Q^{-1}) - P$, $A_2 = (B_2 Q^{-1}) - P$ and $A_3 = (B_3 Q^{-1}) - P$.

$$A_1 = \begin{bmatrix} 79 & -94 & 123 \\ 76 & -113 & 143 \\ 93 & -124 & 161 \end{bmatrix} \begin{bmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{bmatrix}^{-1} - P$$

$$A_1 = \begin{bmatrix} 21 & 8 & 7 \\ 16 & 14 & 23 \\ 19 & 18 & 13 \end{bmatrix} - \begin{bmatrix} 1 & 0 & -2 \\ 2 & 3 & -4 \\ 3 & 3 & -6 \end{bmatrix}$$

$$A_1 = \begin{bmatrix} 20 & 8 & 9 \\ 14 & 11 & 27 \\ 16 & 15 & 19 \end{bmatrix}.$$

$$A_2 = \begin{bmatrix} 70 & -97 & 127 \\ 88 & -119 & 151 \\ 31 & -60 & 73 \end{bmatrix} \begin{bmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{bmatrix}^{-1} - P$$

$$A_2 = \begin{bmatrix} 10 & 20 & 7 \\ 24 & 8 & 23 \\ 5 & 8 & 21 \end{bmatrix} - \begin{bmatrix} 1 & 0 & -2 \\ 2 & 3 & -4 \\ 3 & 3 & -6 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} 9 & 20 & 9 \\ 22 & 5 & 27 \\ 2 & 5 & 27 \end{bmatrix}.$$

$$A_3 = \begin{bmatrix} 81 & -113 & 145 \\ 79 & -107 & 141 \\ 91 & -120 & 153 \end{bmatrix} \begin{bmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{bmatrix}^{-1} - P$$

$$A_3 = \begin{bmatrix} 17 & 15 & 17 \\ 11 & 23 & 5 \\ 25 & 8 & 21 \end{bmatrix} - \begin{bmatrix} 1 & 0 & -2 \\ 2 & 3 & -4 \\ 3 & 3 & -6 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 16 & 15 & 19 \\ 9 & 20 & 9 \\ 22 & 5 & 27 \end{bmatrix}.$$

Now converting A_1,A_2 andA_3 to blocks and then into characters we get the origina original message as

“THINK POSITIVE BE POSITIVE”.

ILLUSTRATION 2:

Let n = 4 then each block contain n^2 = 16 characters.

Let the plaintext be **“GOD IS THE SAVIOUR”.**

Converting the message into blocks , we get two blocks containing 16 characters of each.

“GOD#IS#THE#SAVIO” , “UR##############” where ‘#’ stands for empty space and padding is also done for the empty spaces.

Converting to numbers and forming square matrix of order 4 , we get the matrices of plaintext as

$$A_1 = \begin{bmatrix} 7 & 15 & 4 & 27 \\ 9 & 19 & 27 & 20 \\ 8 & 5 & 27 & 19 \\ 1 & 22 & 9 & 15 \end{bmatrix} \quad \text{and}$$

$$A_2 = \begin{bmatrix} 21 & 18 & 27 & 27 \\ 27 & 27 & 27 & 27 \\ 27 & 27 & 27 & 27 \\ 27 & 27 & 27 & 27 \end{bmatrix}$$

Let $P = \begin{bmatrix}1&2&3&-1\\-2&-1&-3&-1\\1&0&1&1\\0&1&1&-1\end{bmatrix}$ and $Q = \begin{bmatrix}3&-2&0&-1\\0&2&2&1\\1&-2&-3&2\\0&1&2&1\end{bmatrix}$ be the keys where Q is a non-singular matrix.

Encryption

The matrices of the ciphertext B_1, B_2 are obtained by $B_1 = (A_1 + P)Q$ and $B_2 = (A_2 + P)Q$

$$B_1 = \left(\begin{bmatrix}7&15&4&27\\9&19&27&20\\8&5&27&19\\1&22&9&15\end{bmatrix} + \begin{bmatrix}1&2&3&-1\\-2&-1&-3&-1\\1&0&1&1\\0&1&1&-1\end{bmatrix}\right)Q$$

$$B_1 = \begin{bmatrix}8&17&7&26\\7&18&24&19\\9&5&28&20\\1&23&10&14\end{bmatrix}\begin{bmatrix}3&-2&0&-1\\0&2&2&1\\1&-2&-3&2\\0&1&2&1\end{bmatrix}$$

$$B_1 = \begin{bmatrix}31&30&65&49\\45&-7&2&78\\55&-44&-34&72\\13&38&44&56\end{bmatrix}$$ and

$$B_2 = \left(\begin{bmatrix}21&18&27&27\\27&27&27&27\\27&27&27&27\\27&27&27&27\end{bmatrix} + \begin{bmatrix}1&2&3&-1\\-2&-1&-3&-1\\1&0&1&1\\0&1&1&-1\end{bmatrix}\right)Q$$

$$B_2 = \begin{bmatrix}22&20&30&26\\25&26&24&26\\28&27&28&28\\27&28&28&26\end{bmatrix}\begin{bmatrix}3&-2&0&-1\\0&2&2&1\\1&-2&-3&2\\0&1&2&1\end{bmatrix}$$

$$B_2 = \begin{bmatrix}96&-38&2&84\\99&-20&32&75\\112&-30&26&83\\109&-28&24&83\end{bmatrix}.$$

Decryption

The matrices of the plaintext A_1 *and* A_2 are obtained using $A_1 = (B_1Q^{-1}) - P$ and $A_2 = (B_2Q^{-1}) - P$.

$$A_1 = \begin{bmatrix}31&30&65&49\\45&-7&2&78\\55&-44&-34&72\\13&38&44&56\end{bmatrix}\begin{bmatrix}3&-2&0&-1\\0&2&2&1\\1&-2&-3&2\\0&1&2&1\end{bmatrix}^{-1} - P$$

$$A_1 = \begin{bmatrix}8&17&7&26\\7&18&24&19\\9&5&28&20\\1&23&10&14\end{bmatrix} - \begin{bmatrix}1&2&3&-1\\-2&-1&-3&-1\\1&0&1&1\\0&1&1&-1\end{bmatrix}$$

$$A_1 = \begin{bmatrix}7&15&4&27\\9&19&27&20\\8&5&27&19\\1&22&9&15\end{bmatrix}.$$

$$A_2 = \begin{bmatrix}96&-38&2&84\\99&-20&32&75\\112&-30&26&83\\109&-28&24&83\end{bmatrix}\begin{bmatrix}3&-2&0&-1\\0&2&2&1\\1&-2&-3&2\\0&1&2&1\end{bmatrix}^{-1} - P$$

$$A_2 = \begin{bmatrix}22&20&30&26\\25&26&24&26\\28&27&28&28\\27&28&28&26\end{bmatrix} - \begin{bmatrix}1&2&3&-1\\-2&-1&-3&-1\\1&0&1&1\\0&1&1&-1\end{bmatrix}$$

$$A_2 = \begin{bmatrix}21&18&27&27\\27&27&27&27\\27&27&27&27\\22&27&27&27\end{bmatrix}.$$

Now converting A_1 *and* A_2 to blocks and then into characters we get the original message as

“GOD IS THE SAVIOUR”.

3. CONCLUSION

In this paper, the novel block Hill cipher represents a notable advancement in cryptographic techniques, providing improved security, versatility, and efficiency. Its block-based approach and mathematical operations make it a promising solution for various applications that require secure communication and data protection.

REFERENCES

1. Neha Sharma , Sachin Chirgaiya, A novel approach to Hill Cipher . International journal of Computer Applications 2014; Vol.(108), No (11) ,34-37.
2. W. Stallings , Cryptography and Network Security , 4th edition . Prentice Hall;2005.
3. Y. Kumar , R. Munjal , Dan H Sharma, “ Comparison of symmetric and Asymmetric Cryptography with existing Vulnerabilities and Countermeasures,” International Journal of Computer. Sci .Manag.Stud.,vol. 11, no. 3 , hal .60-63,2011.
4. L.S . Hill , Cryptography in An Algebraic Alphabet, The American Mathematical Monthly ,1929;306-12.
5. Bibhudendra , A novel methods of generating self invertible matrix for hill cipher algorithm . Int. J. Secur., 1: 14-21.,2006.
6. P. Shanmugam and C. Loganathan , Involutory Matrix In Cryptography ,IJRRAS Vol 6,Issue 4,424-428,2011.