International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 581-588
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

# A New variant of Hill Cipher Algorithm for Data Security

**Kalaichelvi V, Manimozhi K, Meenakshi P, Rajakumar B, Vimaladevi P**

**SASTRA University, Kumbakonam, India**

**E-mail :** kalaichelvi2k@src.sastra.edu

## Abstract

Security is the notion of keeping information securely by protecting it from unauthorized users. Cryptography is one of the technologies which will provide security to the data. This paper proposes a new variant of Hill cipher encryption algorithm to provide data security. Generally, Traditional Hill cipher algorithm will encrypt only the alphabets not other text information. The main weakness of this is that it encrypts identical plaintext blocks to identical cipher text blocks. To overcome these issues, the proposed system can be used to encrypt and decrypt any type of messages not only the alphabets. Moreover, Radix 64 conversion eliminates the redundant data occurred in the plain text pattern. So, it improves the complexity of cipher text.

**Keywords:** Hill Cipher, Security, Cryptography, Radix 64 Conversion

## 1.0 Introduction

Now-a-days, Human life is integrated with the world through network. Hush-hushes of information are transmitted through the network for every second. So, there we need to provide security. Cryptography is one of the technologies which will provide security to the data. Generally, the Cryptosystem is classified into two broad categories such as Symmetric Key Cryptosystem and Public Key Cryptosystem. In Symmetric Key Cryptosystem, both the sender and receiver will use the same key for encryption and decryption. But, in Asymmetric Key Cryptosystem, different keys are for encryption and decryption. All Symmetric key algorithms are based on the Substitution-Permutation Network (SPN). In Substitution technique, each symbol is replaced by other symbol and in Transposition technique, positions of the symbols in the input are interchanged. Many techniques have been developed based on this Substitution and Transposition like Ceasar Cipher, Playfair Cipher, Hill Cipher, Mono alphabetic, Poly alphabetic, One-time pad, Rail-fence and Single column transposition, etc., One of the classical encryption technique is Hill Cipher. The Traditional Hill Cipher is one of the multi-letter encryption cipher which was developed by Lester. S. Hill in 1929. The Traditional Hill Cipher algorithm will encrypt only the alphabets. We cannot encrypt the plaintext other than the alphabets. To overcome this discrepancy, this paper proposes a new adaptable hill cipher algorithm using Radix 64 conversion.

The organization of the paper is as follows. Section 2 discuss about the various research papers related to Hill cipher algorithm. Basic concepts of the traditional Hill cipher algorithm and Radix 64 conversion are outlined in section 3. Section 4 discusses about the Proposed Hill cipher algorithm for encryption / decryption methods are presented with examples. Finally, section 5 describes the concluding remarks.

## 2.0 Literature Survey

Hill Cipher is one of the poly alphabetic cipher based on linear algebra. Several researches have been done to improve the security of Hill Cipher. Some of the papers have been discussed in this section.

Ismail et al., The main limitation with Hill Cipher is that it is prone to a known plaintext attack, that is, if an attacker has distinct plaintext and cipher text pairs then they retrieve the key by solving depending on the encryption equation used [1]. Rushdi et al. also noticed the problem of non invertible matrix key in Hill cipher. They designed a robust cryptosystem algorithm for non invertible matrices. The non invertible matrix key problem is solved by converting each plaintext character into two cipher text characters. The drawback of this algorithm is transmission of 2n characters is required to encrypt n characters [2]. Yi-Shiung Yeh et al., presented a new polygraph substitution algorithm based on different bases. Their algorithm uses two coprime base numbers that are securely shared between the participants. The main drawback of this paper is that it is time consuming and is not efficient for dealing bulk data [3]. Chefranov et.al., [5] proposed a modification to [4] that works similar to Hill cipher permutation method, but it does not transfer permutation vector, instead both sides use a pseudo-random permutation generator, and only the number of the necessary permutation is transferred to the receiver. The number of dynamic keys is the same as [4]

## 3.0 Traditional Hill Cipher Algorithm:

The Hill cipher algorithm is a polygraphic substitution cipher algorithm based on linear transformation, and is invented by Lester S. Hill in 1929. For encryption, algorithm takes *m* successive plaintext letters and instead of that substitutes *m* cipher letters. In Hill cipher, each character is assigned a numerical value (like *a* = 0, *b* =1, ... , *z* = 25). The substitution of cipher text letters in the place of plaintext letters leads to *m* linear equation.

Encryption can be performed by using the following equation.

**C = KP mod 26**

Decryption requires the inverse of the matrix K. The inverse matrix $K^{-1}$ of a matrix K is defined by the equation $\mathbf{KK^{-1}=K^{-1}K=I}$, where I is the Identity matrix.

In general term we can write as follows:

$\mathbf{P = K^{-1}C \bmod 26}$

### 3.1 Radix 64 Conversion

Radix 64 conversion is a binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. Radix 64 conversion table uses 65 characters. It consists of 26 Uppercase letters, 26 Lower case letters, 10 digits and 2 special characters i.e., + and / and a padding character (‘=’). So, totally it contains 65 characters. Radix 64 encoding and decoding procedure is used in both encryption and decryption side. It takes 3 characters at a time and then it is converted into binary based on the ASCII value of the characters. So, we will get totally 24 bits. These 24 bits are divided into *four* groups of 6 bits and find the corresponding decimal value. Finally, pick the corresponding Radix 64 character from the Radix 64 conversion table. Radix 64 decoding is the reverse process of Radix 64 encoding procedure.

## 4.0 Proposed Methodology:

The Traditional Hill cipher algorithm is one of the symmetric key algorithms that have several advantages in data encryption. However, a main drawback of this is that it encrypts identical plaintext blocks to identical cipher text blocks. Moreover, it will encrypt only the alphabets. To overcome the above said problems, this paper recommends a new variant of Hill cipher algorithm for encryption and decryption. Using this proposed system [Fig.1], we can encrypt any type of message like digits, special characters, special symbols, etc.,

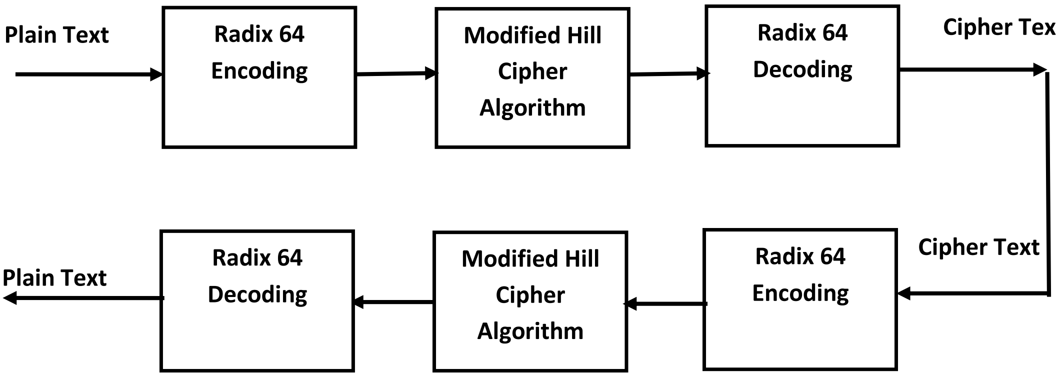

**Fig.1. Proposed Hill Cipher Algorithm**

**Encryption:**

1. Read the Plaintext from file.
2. Convert the Plaintext into Radix 64 Characters by applying Radix 64 Encoding.
3. Then, Radix 64 characters are converted into some values using the proposed Hill Cipher algorithm with the help of key..
4. Finally, these values are converted into Cipher text by applying Radix 64 Decoding.

**Decryption:**

1. Read the Cipher text from file.
2. Convert the Cipher text into Radix 64 characters using Radix 64 Encoding.
3. Then, Radix 64 characters are converted into some values using the proposed Hill Cipher algorithm with the help of Inverse Key. So, the receiver, should find Inverse key prior to this step.
4. Finally, these values are converted into Plaintext by applying Radix 64 Decoding.

### 4.1 Illustration

**PlainText : **CRYPTO

| | | | | |
|---|---|---|---|---|
| **01000011** | **01010010** | **01011001** | | **(8-bit Binary value of C R Y)** |
| **010000** | **110101** | **001001** | **011001** | |
| **16** | **53** | **9** | **25** | **(Radix 64 value)** |
| Q | 1 | J | Z | **(Radix 64 Characters)** |

Once the Plain text characters are converted into Radix 64 characters and then only the Radix 64 characters are encrypted using Modified Hill Cipher algorithm.

Consider **K** = $\begin{pmatrix} 32 & 13 & 41 \\ 49 & 11 & 22 \\ 31 & 53 & 61 \end{pmatrix}$

**Encryption:**

**C=KP Mod 64**

$$\Rightarrow \begin{pmatrix} 9 & 4 & 3 \\ 21 & 33 & 17 \\ 16 & 27 & 11 \end{pmatrix} \begin{pmatrix} 16 \\ 53 \\ 9 \end{pmatrix} \text{ Mod } 64$$

$$\Rightarrow \begin{pmatrix} 63 \\ 62 \\ 58 \end{pmatrix} \Rightarrow \begin{pmatrix} / \\ + \\ 6 \end{pmatrix}$$

**(Corresponding Radix 64 Characters)**

Similarly, the other characters are in the Plain text converted into Radix 64 characters. Finally, Radix 64 decoding is applied to get the equivalent ASCII characters as a final Cipher text.

**Decryption:**

$$\mathbf{P} = \mathbf{K}^{-1}\,\mathbf{C}$$

$$\mathbf{K}^{-1} = \begin{pmatrix} 9 & 4 & 3 \\ 21 & 33 & 17 \\ 16 & 27 & 11 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 32 & 13 & 41 \\ 49 & 11 & 22 \\ 31 & 53 & 61 \end{pmatrix} \begin{pmatrix} 63 \\ 62 \\ 58 \end{pmatrix} \text{ Mod } 64$$

$$\rightarrow \begin{bmatrix} \mathbf{16} \\ \mathbf{53} \\ \mathbf{9} \end{bmatrix} \rightarrow \begin{bmatrix} \mathbf{Q} \\ \mathbf{1} \\ \mathbf{J} \end{bmatrix} \quad \textbf{(Corresponding Radix 64 Characters)}$$

Similarly, the other characters are in the Cipher text converted into Radix 64 characters. Finally, Radix 64 decoding is applied to get the equivalent ASCII characters as a final Plain text.

## 5.0 Conclusion

In this paper, we have pointed the traditional Hill cipher algorithm and its drawbacks. In order to overcome the issues, we have proposed an extension to traditional Hill cipher algorithm that can be used more efficiently. The proposed system can be used to encrypt and decrypt any type of messages not only the alphabets. Moreover, Radix 64 conversion eliminates the redundant data occurred in the plain text pattern. So, it improves the complexity of cipher text.

## References

1. Ismail I A, Amin Mohammed, Diab Hossam, How to Repair the Hill Cipher, Journal of Zhejiang University Science, 7(12), pp. 2022-2030, 2006.
2. A. H. Rushdi and F. Mousa, “Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher ”Intl Journal of Computer Science and Network Security , vol.9, no.5, 2009 pp. 11-16
3. Yeh YS, Wu TC, Chang CC, Yang WC. “A New Cryptosystem Using Matrix Transformation”. 25th IEEE International Carnahan Conference on Security Technology 1991: 131-138
4. Chefranov A. G., “Secure Hill Cipher Modification SHC-M” Proc. Of the First International Conference on Security of Information and Network (SIN2007) 7-10 May 2007, Gazimagusa (TRNC) North Cyprus, Elci, A., Ors, B., and Preneel, B (Eds) Trafford Publishing, Canada, 2008: pp 34-37, 2007
5. Y. Mahmoud Ahmed, Chefranov A. G., “ Hill Cipher Modification Based on Pseudo-Random Eigen values HCM-PRE” Submitted to Turkish Journal of Electrical Engineering & Computer Science on 2-03-2010
6. William Stallings, “Cryptography and Network Security”, 5th Edition.
7. Bruce Schneier, "Applied Cryptography" , John Wiley & Sons, Inc 1996
8. Richard Smith "Internet Cryptography",Pearson Edn Pvt.Ltd
9. Atul Kahate “Cryptography and Network Security”, Tata Mc.Graw Hill

10. RAJESH, M. "A SYSTEMATIC REVIEW OF CLOUD SECURITY CHALLENGES IN HIGHER EDUCATION." The Online Journal of Distance Education and e- Learning 5.4 (2017): 1.
11. Rajesh, M., and J. M. Gnanasekar. "Protected Routing in Wireless Sensor Networks: A study on Aimed at Circulation." Computer Engineering and Intelligent Systems 6.8: 24-26.
12. Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous WANET using FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974 (2015): 2115.
13. Rajesh, M., and J. M. Gnanasekar. "Hop-by-hop Channel-Alert Routing to Congestion Control in Wireless Sensor Networks." Control Theory and Informatics 5.4 (2015): 1-11.
14. Rajesh, M., and J. M. Gnanasekar. "Multiple-Client Information Administration via Forceful Database Prototype Design (FDPD)." IJRESTS 1.1 (2015): 1-6.
15. Rajesh, M. "Control Plan transmit to Congestion Control for AdHoc Networks." Universal Journal of Management & Information Technology (UJMIT) 1 (2016): 8-11.
16. Rajesh, M., and J. M. Gnanasekar. "Consistently neighbor detection for MANET." Communication and Electronics Systems (ICCES), International Conference on. IEEE, 2016.