Hill Cipher Key Generation Algorithm by using Orthogonal Matrix

Fozia Hanif Khan, Rehan Shams, Farheen Qazi, Dure-E-ShawarAgha

Abstract— The role of cryptography in today's world is significant. It secures information mathematically by mailing massage with a key. Hill cipher is one of the most famous symmetric cryptosystem that can be used to protect information from unauthorized access. This paper suggest a new technique in Hill cipher, here we are establishing the complex procedure of key generation for the process of encryption. This paper explains how the orthogonal matrix can be useful for the generating the key matrix in Hill cipher. Hill cipher is a matrix based poly-graphic substitution. For example {abcd}= ab cd ef… or abc def…and so on. The purpose of generating the key by using orthogonal matrix is to overcome the disadvantage of non invertible matrix in Hill cipher. This paper discovers the idea of generating key that is basically the reflection on a given plane in $\mathbb{R}^3$. The proposed concept is very easy to implement but it will be more difficult for the attacker to get the key.

Keywords — Hill cipher, Network security, Cryptography, orthogonal matrix.

I. INTRODUCTION

People all over the world are engaged in communication through internet every day. It is very important to secure our essential documents from unauthorized users. Hence network security is looming on the horizon as a potentially massive problem. Various algorithm have been made in this field but, each of them have their own merits and demerits. As a result researchers are trying to explore new techniques in the field of cryptography to enhance the network based security further. The data transferred from one system to another system over the public network can be protected by means of encryption. On encryption the data is encrypted by the algorithm using the 'key'. Only the user having the access to the same 'key' can decrypt the data. Cryptography not only allows individuals to keep their communications records secret, it allows them to keep their identities secret. Hill cipher is an application of linear algebra to cryptography (the science of making and breaking code and ciphers). The core of Hill cipher is a matrix manipulation. It is a multi-letter cipher developed by the mathematician Laster Hill in 1929. Hill cipher is a poly-graphic substitution cipher based on linear algebra.

Manuscript Received on January 2015.

Fozia Hanif Khan, Department of Mathematics Sir Syed University of Engineering and Technology, Karachi, Pakistan.

Rehan Shams, Department of Telecommunication Sir Syed University of Engineering and Technology, Karachi, Pakistan.

Farheen Qazi, Department of Computer Engineering Sir Syed University of Engineering and Technology, Karachi, Pakistan.

Dure-e-ShawarAgha, Department of Computer Engineering Sir Syed University of Engineering and Technology, Karachi, Pakistan.

Hill's major contribution was the use of mathematics to design and analyses cryptosystem . Our paper suggest the enhancement of Hill cipher against the known plain text attack because of the symmetric cryptosystem. For symmetric key-based encryption the same key is used for decryption. The disadvantage of symmetric key is that, it only requires a single key to break the encryption . For that particular reason the key must be well secured and protected. This key is often called a secrete key. Many symmetric key algorithms have been constructed like substitution box, also known as S-box. Several improvisation have been done, regarding the Hill cipher, playfair and Vigenere ciper [10], all have improve the communication security. In [5] there is a modification of Hill cipher by using randomized approach, [3] has done the extension of playfair cipher of 16×16 matrix, also [8] has made a new model of Hill cipher by using quadratic residues, [1] has developed the universal playfair cipher using m×n matrix, [6] has establishes the concept of bit level block encoding technique using symmetric key cryptography to enhance the security of network based transmission. Considering the methodology in which for encryption algorithm m successive plaintext letters are used instead of that substitutes m cipher letters. In Hill cipher each character is assigned a numerical values like a=1, b=2…….z=26. As explained earlier, it requires the key matrix and its inverse in hill cipher encryption and decryption respectively. Therefore one problem arises that what happens when the inverse of the matrix does not exist? If it is not so then how the decryption takes place. In order to overcome all the above discussed difficulties this paper establishes the idea of taking the orthogonal matrix as a key for the encryption but for the security measures the key matrix will not be disclose to the sender. The receiver will find the "key", which is actually the orthogonal matrix (in standard basis) that implements reflection on the plane and that equation will be provided by the sender to generate the key. Many users have overcome these difficulties by applying different procedures such as the technique of self repetitive matrix. But the presented algorithm is easy to implement and will make it more secure as far as the key generation step is concerned.

II. ORTHOGONAL MATRIX

A. Defination

As far as the description of orthogonal matrix is concern, a matrix A is called orthogonal if A preserve length of vectors, that is if.

(Av, Av) = (v, v) For all vectors v in $\mathfrak{R}^n$ (1)

An orthogonal n×n matrix is the n- dimensional analogue of the rotation matrices $\mathbf{R_o}$ in $\mathbf{R^2}$. When does a linear transformation of $\mathfrak{R}^2$ (or $\mathfrak{R}^3$) deserve to be called a rotation? Rotations are rigid motions in the geometric sense of preserving the length of vectors and the angle between vectors.

B. Properties

An n×n matrix is said to be orthogonal if $\mathbf{A^tA=I_n}$, $\Rightarrow \mathbf{A^t = A^{-1}}$, from the basic property of the transpose (for any A)

Av. w = v A^t w, $\forall$ v, w $\in\mathfrak{R}^n$

Av. Aw= v.w, $\forall$ v, w $\in\mathfrak{R}^n$

v A^t Aw= v.w, $\forall$ v, w $\in\mathfrak{R}^n$

A matrix is orthogonal matrix exactly when its column vectors have length one, and are pair wise orthogonal , like wise for the row vectors, in short, the column (or the rows) of an orthogonal ,matrix are orthogonal basis of $\mathfrak{R}^n$.

Any orthogonal matrix is invertible with $A^{-1}= A^t$, if A is orthogonal so are A^t and A^{-1}.

The purpose of using the orthogonal matrix in hill cipher procedure is to make the massage more secure and protected. Regarding the fact that only sender and receiver knows about the secrete that the key matrix is supposed to be the orthogonal matrix that implements reflection on the given plan in $\mathfrak{R}^n$.

C. Reflections:

A linear transformation T of $\mathfrak{R}^n$ is a reflection if there is one-dimensional subspace L (a line through 0) so that,

T v = -v for v$\in$ L and T v= v for v in the orthogonal complement $L^{\perp}$. Letting n be a unit vector spanning L, we find the expression for T_v:

T_v = v-2 (v. n) n, v$\in\mathfrak{R}^n$ (2)

If $\{v_1 \ldots\ldots v_{n-1}\}$ is a basis of L, in the B= { \, $\subseteq_\infty$, …..$\subseteq_\infty$} of $\mathbb{R}^n$. The matrix of the reflection key take the form (for n=3)

$$[T_B]=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} \quad (3)$$

If a is a number then a^{-1} is called the reciprocal or multiplicative inverse of a module 26 if $aa^{-1}= a^{-1}a=1$ mod 26.

III. ALGORITHM FOR ENCRYPTION

i. Divide the given plane text in to equal part such that length of each part is equivalent to the dimension of the given equation.

ii. Generate the initial cipher text from the plain text using ordinary Hill cipher procedure.

iii. Generate the key from the given equation of plane by using (2) [11]. Since the key matrix is orthogonal therefore we must have the fraction value in the calculated key matrix. Replace these fraction value by using the multiplicative inverse in the mod 26.

iv. Multiply the key matrix along with negative values with the converted cipher text matrix. After multiplication consider the remainder in the mod 26 and construct the new encrypted text.

IV. ALGORITHM FOR THE ENCRYPTION AND DECRYPTION

A. Encryption

By considering the orthogonal matrix as a key matrix for the encryption, and according to the earlier described definition of orthogonal matrix. Take the transpose of the key matrix as a inverse. For the encryption we take m successive plane letters. Hill cipher developed a block cipher, the encryption of which is described by the equation.

C ≡ KP mod 26 (3)

Where K is the key matrix obtained by using the equation (2) of size n×n, P is the plain text and C is the cipher text both having n components.

For m=3the system can be described as follows,

$$\begin{bmatrix}C_1\\ C_2\\ C_3\end{bmatrix} \equiv \begin{bmatrix}K_{11} & K_{12} & K_{13}\\ K_{21} & K_{22} & K_{23}\\ K_{31} & K_{32} & K_{33}\end{bmatrix}\begin{bmatrix}P_1\\ P_2\\ P_3\end{bmatrix} mod\ 26 \quad (4)$$

Where C and P are column vectors of length 3, representation the plain text and the transferred matrix, and K is the is a 3×3 matrix.

B. Decryption

Find the Inverse of the key matrix K and applied to the transferred matrix C with respect to mod 26, then plain text is recovered.

V. GENERATION OF KEY FROM THE EQUATION

A. Example

Consider the plane with an equation

$2x_1 + 3x_2 + x_3 = 0$ (5)

The orthogonal line L is spanned by the unit vector n= $\frac{1}{\sqrt{14}}(2, 3, 1)$

From (2) we have,

$$T_v = v\text{-}2\,\frac{1}{14}\langle v,\ (2,3,1)\rangle\,(2,3,1)$$

by taking,

$$T_{v_1} = (1,0,0) - \frac{4}{14}(2, 3, 1)$$

$$T_{v_2} = (0,1,0) - \frac{6}{14}(2, 3, 1)$$

$$T_{v_3} = (0,0,1) - \frac{2}{14}(2, 3, 1)$$

And the orthogonal matrix $T_{\perp}$ from the above equation will be

$$T_{\perp} = \frac{1}{7}\begin{bmatrix}3 & -2 & -6\\ -2 & 6 & -3\\ -6 & -3 & -2\end{bmatrix}$$

$$T_{\perp} = 15\begin{bmatrix}3 & -2 & -6\\ -2 & 6 & -3\\ -6 & -3 & -2\end{bmatrix}$$

since the multiplicative inverse of 7 is equal to 15 in the mod 26.For encryption the receiver has to calculate this above matrix to decrypt the data, in mod 26. Therefore, the above key matrix will become,

$$K = \begin{bmatrix}45 & -30 & -90\\ -30 & 90 & -45\\ -90 & -45 & -30\end{bmatrix}$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

For the given massage let's suppose we have,
Herbert Yardley wrote the American Black Chamber:
According to the procedure of Hill cipher break the massage in to equal parts:

her ber tya rdl eyw rot eth eam eri can cha mbe …

for completing the pair we would place a null at the end. Now convert the above letters in to numbers by using a=01, …….z=26, Now we have following pairs in numbers,

8518 2518 20251 18412 52523 181520 851 13518 931 14212 13113 1132 5180

Now we encrypt each pair by using the above key in such a way that each pair will become a column vector h(8) e(5) r(18), by using the equation (4).

$$\begin{bmatrix} 45 & -30 & -90 \\ -30 & 90 & -45 \\ -90 & -45 & -30 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \\ 18 \end{bmatrix} = \begin{bmatrix} -1410 \\ -600 \\ -1485 \end{bmatrix}$$

We need our result to be mod 26

$$\begin{bmatrix} -1410 \\ -600 \\ -1485 \end{bmatrix} = \begin{bmatrix} 6 \\ 2 \\ 3 \end{bmatrix} \text{mod } 26$$

The new text will become, f(6) b(2) c(3),

We continue to do this and obtained the coded text, but for the decryption the receiver doesn't need to calculate the inverse of key matrix just take the transpose of the orthogonal matrix and decode in the same manner, that is multiplying the coded text with the key matrix and get the original text.

$$A^{-1} = \begin{bmatrix} 45 & -30 & -90 \\ -30 & 90 & -45 \\ -90 & -45 & -30 \end{bmatrix}$$

Which is supposed to be equal in most of the time.

$$\begin{bmatrix} 45 & -30 & -90 \\ -30 & 90 & -45 \\ -90 & -45 & -30 \end{bmatrix} \begin{bmatrix} 6 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} -60 \\ -135 \\ -720 \end{bmatrix} 26 = \begin{bmatrix} 8 \\ 5 \\ 18 \end{bmatrix}$$

VI. CONCLUSION

In the given work the key matrix of classical Hill cipher is modified in order to increase the security of communication text. Since the improvisation of cipher text made in this paper is relatively more secure due to the utilization of orthogonal matrix which is actually generated from the equation of plane. The concept of sending the equation has made the whole procedure much protected.

REFERENCES

1. Alam A., Sehat ullah, Itiaq W., Khalid S., (2011), International journal of advance computer science, Vol. 1, No. 3, pp. 113-117.
2. David S., (2008), " The playfair cipher" Vinculum Vol. 45, No. 2, pp. 4-6.
3. Dhenakaran S. S., Llayaraja M., (2012)"Extansion of Playfair Cipher usinf 16×16 Matix", International Journal of computer, Vol. 48, No. 7, pp. 37-41.
4. Hassan. H. A., Seab M., and Hameed H. D., (2005), " The Pyramids of Block Cipher", International Journal of Network Security. Vol.1, No. 1, PP. 52-60.
5. Krishna A. V. N., Madhuravani K., (2012), "A Modified Hill cipher using Randamized Approach" I. J. Computer Network and Information Security, No. 5, 56-62.
6. Manas P., Jyotsna K., (2012), " A General Session Based a Bit Level Block Encoding Technique using Symmetric key Cryptography to enhance the security of Network Based Transmission", International Journal of computer science, Engineering and Information Technolgy, Vol. 2, No. 3, pp. 31-42.
7. Michael A., (1995), The Metaphor is the key: Cryptography, the Clipper chip and the Constitution, University of Pennsylvania law Review, Vol. 143, No. 3.
8. Rushdi A., Farajallah M., (2009), " A Design os a roust cryptosystem algorithm for Non- Invertable Matrices Based on Hill cipher", International journal of computer science and Network Security, Vol. 9, pp. 11-16.
9. Sreenivasulu R., Murali S., (2012), International Journal of computer science and information technology, Vol. 2, No. 1, pp. 121-124.
10. Sivagurunathan G., Rajendran V., (2010), "Classification of Substitution Cipher using Neural Networks", International Journal of computer science and network Security, Vol. 10, No. 3, pp. 274-279.
11. *www.math.utk.edu/~freire/teaching/.../m251s10orthogonal.pdf*