ISSN: 0975-766X
CODEN: IJPTFI
*Available Online through* *Research Article*
**www.ijptonline.com**

# GENERALIZED SELF-INVERTIBLEKEY GENERATION ALGORITHM BY USING REFLECTION MATRIX IN HILL CIPHER AND AFFINE HILL CIPHER

**M .G .Vara Prasad[1], P. Sundarayya[2]**
[1]Department ofmathematics, NSRIT, India.
[2]Department of Engineering Mathematics, GITAM University, India.
*Email: prasadvaram11@gmail.com*

*Received on: 15.10.2016* *Accepted on: 12.11.2016*

**Abstract**

In this paper discover the idea of generating generalizedself-invertible reflection matrix key in Hill Cipher and Affine Hill Cipher. The inverse of the matrix used for encrypting the plaintext does not consistently exist. So, if the matrix is not invertible, the encrypted cipher text content cannot be decrypted. In the generalized self-invertible matrix generation method, the key matrix used for the encryption is itself self-invertible. So, we need not find the inverse of the matrix at the time of decryption. Moreover, this method eliminates the computational complexity involved in finding the inverse of the matrix while decryption and this method more secure due togenerate generalized self-invertible key matrix using a homogeneous linear equation under modulation of a prime number.

## 1. Introduction

The Hill cipher was invented by L.S. Hill in 1929 [1]. Hill cipher is a one of the classical substitution technique that has been developed based on linear transformation. It has both advantages and drawbacks. The main advantages are disguising letter frequencies of the plaintext; high speed, high throughput, and the simplicity because of using matrix multiplication and inversion for enciphering and deciphering. The disadvantages are, it is vulnerable to known plaintext attack and the inverse of the shared key matrix may not exist always. To overcome the drawbacks of Hill cipher algorithm many modifications are presented. In this proposed work generating matrix key this is self-invertible using same key in the process of encryption and decryption in Hill Cipher & Affine Hill Cipher under modulation of prime number.

## 2. The Hill Cipher

In the Hill cipher, the cipher text is obtained from the plaintext by means of a linear transformation. The plaintext column vector **R**is encrypted as **S=KR**(mod m) in which **S**is the cipher text column vector, **K** is an n×n key matrix

where $k_{ij} \in$ in which $Z_m$ is ring of integers modulo m where m is a natural number that is greater than one. The encryption procedure proceeds by encoding the resulted cipher text row vector into alphabets of the main plaintext. The value of the modulus m in the original Hill cipher was 26 but its value can be optionally selected. The key matrix **K** is supposed to be securely shared between the participants. The cipher text **R** is decrypted as $\mathbf{R} = \mathbf{K}^{-1}\mathbf{S} \pmod m$. All operations are performed over $Z_m$. For decryption to be possible, the key matrix **K** should be invertible or equivalently, it should satisfy gcd (det **K**(mod m), m) = 1 [2]. However, many of square matrices are not invertible over $Z_m$. The risk of determinant having common factors with the modulus can be reduced by taking a prime number as the modulus such selection also increases the key space of the cryptosystem [8].

Encryption:

$$S=\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix} R \pmod m$$

Decryption:

$$R=\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix}^{-1} S \pmod m$$

**3. The Affine Hill Cipher**

The Affine Hill cipher extends the concept of Hill cipher by mixing it with a nonlinear affine transformation [2]. The Affine Hill cipher is an application linear algebra. It is one the block cipher to encrypt and decrypt the messages using matrix key and its inverse and it is a symmetric key algorithm. So the encryption expression will have the form of $\mathbf{S} = (\mathbf{KR} + \mathbf{T}) \pmod m$ . All operations are performed over $Z_m$.Where B is column vector over $Z_m$. It should satisfy g.c.d (det**K**(mod m), m) = 1

Encryption:

$$S=\left(\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix} R + B\right) \pmod m$$

Decryption:

$$R=\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix}^{-1} (S - B) \pmod m$$

## 5. The Proposed Scheme

**Definition:** Let $\mathbf{n^T} \in \mathcal{R}^m$ with $\mathbf{n}^T\mathbf{.n=1}$then the matrix Kof order m is said to be reflection matrix or house holder's matrix if $K=I_m-2\mathbf{n}.\mathbf{n}^T$Where $I_m$ is identity matrix

Theorem: If $K=I_m-2\mathbf{n}.\mathbf{n}^T$ is reflection matrix then K is symmetric, orthogonal and self-invertible

Proof: Since $K=I_m - 2\mathbf{n}.\mathbf{n^T} \Rightarrow K^T=(I_m - 2\mathbf{n}.\mathbf{n^T})^T \Rightarrow {I_m}^T-2(\mathbf{n}.\mathbf{n^T})^T \Rightarrow I_m - 2(\mathbf{n^T})^T(\mathbf{n^T})$

$\Rightarrow K^T=I_m - 2\mathbf{n}.\mathbf{n^T}= K$

$KK^T=(I_m - 2\mathbf{n}.\mathbf{n^T})(I_m - 2\mathbf{n}.\mathbf{n^T})=I_m - 2\mathbf{n}.\mathbf{n^T} - 2\mathbf{n}.\mathbf{n^T}+4\,\mathbf{n}(\mathbf{n}^T.\mathbf{n})\mathbf{n^T} = I_m - 4\mathbf{n}.\mathbf{n^T} + 4\mathbf{n}.\mathbf{n^T}$

$\therefore\ KK^T = I_m$

$K^T\,K=(I_m - 2\mathbf{n}.\mathbf{n^T})(I_m - 2\mathbf{n}.\mathbf{n^T}) = I_m - 4\mathbf{n}.\mathbf{n^T} + 4\mathbf{n}.\mathbf{n^T} = I_m \therefore KK^T = K^T\,K = I_m$

K is symmetric, orthogonal $K^T = K^{-1}$ and $K^T = K \therefore K^{-1} = K$, K is self-invertible

### 5.1. Generalized Key Generation reflection matrix from a homogenous linear equation$\sum_{i=1}^{m} a_i x_i$=0

A linear homogenous equation $\sum_{i=1}^{m} a_i x_i$=0,Let B be a column normal vector then $B^T=(a_1,a_2,a_3,\ldots\ldots\ldots a_m)$and $\mathbf{n}$ be a unit normal vector of $B^T$ then$\mathbf{n} =\frac{B}{\|B\|}=\frac{1}{\sqrt{\sum_{i=1}^{m} {a_i}^2}}\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$ and

$\mathbf{n^T} = \frac{B^T}{\|B^T\|} = \frac{1}{\sqrt{\sum_{i=1}^{m} {a_i}^2}}(a_1,a_2,\ldots\ldots a_m) \in \mathcal{R}^m$

$\mathbf{n}^T.\mathbf{n} = (\frac{1}{\sum_{i=1}^{m} \mathbf{a_i}^2})(a_1,a_2,\ldots\ldots a_m)\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}=\frac{{a_1}^2+{a_2}^2+\cdots+{a_m}^2}{\sum_{i=1}^{m} \mathbf{a_i}^2} =\frac{\sum_{i=1}^{m} \mathbf{a_i}^2}{\sum_{i=1}^{m} \mathbf{a_i}^2} =1$

$\therefore \mathbf{n^T} \in \mathcal{R}^m$and $\mathbf{n}^T.\mathbf{n} = \mathbf{1}$ Then reflection matrix is $K=I_m - 2\mathbf{n}.\mathbf{n^T}$, Where$I_m$ is identity matrix

$K =I_m - \frac{2}{\sum_{i=1}^{m} \mathbf{a_i}^2}\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}(a_1,a_2,\ldots\ldots a_m)$

$K=\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} - \frac{2}{\sum_{i=1}^{m} \mathbf{a_i}^2}\begin{pmatrix} \mathbf{a_1}^2 & a_1a_2 & \cdots & a_1a_m \\ a_1a_2 & \mathbf{a_2}^2 & \cdots & a_2a_m \\ \cdots & \cdots & \cdots & \cdots \\ a_1a_m & a_2a_m & \cdots & \mathbf{a_m}^2 \end{pmatrix}$

$K=\frac{1}{\sum_{i=1}^{m} \mathbf{a_i}^2}\begin{pmatrix} \sum_{i=1}^{m} \mathbf{a_i}^2 - 2\mathbf{a_1}^2 & -2a_1a_2 & \cdots & -2a_1a_m \\ -2a_1a_2 & \sum_{i=1}^{m} \mathbf{a_i}^2 - 2\mathbf{a_2}^2 & \cdots & -2a_2a_m \\ \cdots & \cdots & \cdots & \cdots \\ -2a_1a_m & -2a_2a_m & \cdots & \sum_{i=1}^{m} \mathbf{a_i}^2 - 2\mathbf{a_m}^2 \end{pmatrix}$

**5.1.1. Generalized reflection matrix key generation algorithm**

- Step1:Input values$a_1, a_2, a_3, \ldots\ldots\ldots a_m \in Z_q$
- Step2:Check g.c.d($\sum_{i=1}^{m} a_i^2$,q)=1
- Step3:Calculate K=$I_m$-2**n**.$\mathbf{n}^T$
- Step4:Calculate K=K(mod q)

**5.1.2. Reflection matrix from the line equation a x +by =0:**

If a x +by=0 be line equation then normal vector $B^T$= (a b) ∴ $\mathbf{n} = \begin{pmatrix} \frac{a}{\sqrt{a^2+b^2}} \\ \frac{b}{\sqrt{a^2+b^2}} \end{pmatrix}$ and $\mathbf{n^T}=\begin{pmatrix} \frac{a}{\sqrt{a^2+b^2}} & \frac{b}{\sqrt{a^2+b^2}} \end{pmatrix}$

Reflection matrix K= $I_2$-2**n**.$\mathbf{n}^T$

Reflection matrix K=$\frac{1}{a^2+b^2}\begin{pmatrix} b^2-a^2 & -2ab \\ -2ab & a^2-b^2 \end{pmatrix}$

**5.1.3. Reflection matrix from the plane equation a x +by +c z=0:**

If the plane equation a x +by +c z=0 then normal vector

$B^T$=(a b c) , **n**=$\begin{pmatrix} \frac{a}{\sqrt{a^2+b^2+c^2}} \\ \frac{b}{\sqrt{a^2+b^2+c^2}} \\ \frac{c}{\sqrt{a^2+b^2+c^2}} \end{pmatrix}$ and $\mathbf{n}^T$=$\begin{pmatrix} \frac{a}{\sqrt{a^2+b^2+c^2}} & \frac{b}{\sqrt{a^2+b^2+c^2}} & \frac{c}{\sqrt{a^2+b^2+c^2}} \end{pmatrix}$

Reflection matrix K= $I_3$-2**n**.$\mathbf{n}^T$

∴K=$\frac{1}{a^2+b^2+c^2}\begin{pmatrix} -a^2+b^2+c^2 & -2ab & -2ca \\ -2ab & a^2-b^2+c^2 & -2bc \\ -2ca & -2bc & a^2+b^2-c^2 \end{pmatrix}$

**5.1.4.Examplefor Key Generation from reflection matrixfrom the plane equation** x+4y+3z=0**:**

Choose q=37 ,$B^T$ =(1 4 3) , **n**=$\begin{pmatrix} \frac{1}{\sqrt{26}} \\ \frac{4}{\sqrt{26}} \\ \frac{3}{\sqrt{26}} \end{pmatrix}$ and $\mathbf{n}^T$=$\begin{pmatrix} \frac{1}{\sqrt{26}} & \frac{4}{\sqrt{26}} & \frac{3}{\sqrt{26}} \end{pmatrix}$

Reflection matrix K= $I_3$-2**n**.$\mathbf{n}^T$

K=$\frac{1}{26}\begin{pmatrix} 24 & -8 & -6 \\ -8 & -6 & -24 \\ -6 & -24 & 8 \end{pmatrix}$

**K**=$\frac{1}{26}\begin{pmatrix} 24 & -8 & -6 \\ -8 & -6 & -24 \\ -6 & -24 & 8 \end{pmatrix} mod\ 37=\begin{pmatrix} 18 & 31 & 14 \\ 31 & 14 & 19 \\ 14 & 19 & 6 \end{pmatrix}$

∴**K**=$\begin{pmatrix} 18 & 31 & 14 \\ 31 & 14 & 19 \\ 14 & 19 & 6 \end{pmatrix}$ and$\mathbf{K^{-1}}=\begin{pmatrix} 18 & 31 & 14 \\ 31 & 14 & 19 \\ 14 & 19 & 6 \end{pmatrix} \in {Z_{37}}^{3\times3}$

**5.2. Proposed technique on Hill Cipher:**

Prime modulus generates large key space than a composite modulus and taking q is prime number.The plaintext column vector **R**is encrypted as **S=KR**(mod q) in which **S**is the cipher text column vector, **K** is an m×mkey matrix where $k_{ij}$∈in which $Z_q$ and The cipher text **R** is decrypted as **R=KS**(modq)where **K**=$I_m$-2**n**.**n**$^T$Where $I_m$ is identity matrix and **n**=$\frac{B}{\|B\|}$.It should satisfyg.c.d (det**K**(mod q), q) = 1.

**5.2.1. Encryption algorithm:**

Step 1: Generate reflection matrix key **K** from reflection matrix key generation algorithm.

Step 2:Calculate **S=KR**(mod q) and Step 3:Write Cipher text

**5.2.2. Decryption algorithm**:

- Step1: Calculate R=KS(mod q)
- Step2:Write Plain text

**5.2.3. Example of Proposed technique on Hill Cipher:**

Consider the Plain text=”GOOGLE”

$R=\begin{pmatrix} G \\ O \\ O \\ G \\ L \\ E \end{pmatrix}$is a block of plain text,$R=\begin{pmatrix} 7 \\ 15 \\ 15 \\ 7 \\ 12 \\ 5 \end{pmatrix}$is block of plain text

Key generation: Let us consider equation$x_1 + 2x_2 + x_3 + x_4 + 2x_5 + x_6 = 0$ from generalized reflection matrix key generation algorithm we get Reflection matrix K= $I_6$-2**n**.**n**$^T$

$$K=\frac{1}{12}\begin{pmatrix} 10 & -4 & -2 & -2 & -4 & -2 \\ -4 & 4 & -4 & -4 & -8 & -4 \\ -2 & -4 & 10 & -2 & -4 & -2 \\ -2 & -4 & -2 & 10 & -4 & -2 \\ -4 & -8 & -4 & -4 & 4 & -4 \\ -2 & -4 & -2 & -2 & -4 & 10 \end{pmatrix} \Rightarrow K=34\begin{pmatrix} 10 & -4 & -2 & -2 & -4 & -2 \\ -4 & 4 & -4 & -4 & -8 & -4 \\ -2 & -4 & 10 & -2 & -4 & -2 \\ -2 & -4 & -2 & 10 & -4 & -2 \\ -4 & -8 & -4 & -4 & 4 & -4 \\ -2 & -4 & -2 & -2 & -4 & 10 \end{pmatrix}$$

**Encryption: S=KR**(mod 37)

$$\mathbf{S}=34\begin{pmatrix} 10 & -4 & -2 & -2 & -4 & -2 \\ -4 & 4 & -4 & -4 & -8 & -4 \\ -2 & -4 & 10 & -2 & -4 & -2 \\ -2 & -4 & -2 & 10 & -4 & -2 \\ -4 & -8 & -4 & -4 & 4 & -4 \\ -2 & -4 & -2 & -2 & -4 & 10 \end{pmatrix}\begin{pmatrix} 7 \\ 15 \\ 15 \\ 7 \\ 12 \\ 5 \end{pmatrix}(mod\ 37) = \begin{pmatrix} 17 \\ 35 \\ 25 \\ 17 \\ 32 \\ 15 \end{pmatrix}$$

Which gives cipher text=”Q8YQ5O”

**Decryption:**R=KS(mod 37)

$$R=34\begin{pmatrix}10 & -4 & -2 & -2 & -4 & -2\\ -4 & 4 & -4 & -4 & -8 & -4\\ -2 & -4 & 10 & -2 & -4 & -2\\ -2 & -4 & -2 & 10 & -4 & -2\\ -4 & -8 & -4 & -4 & 4 & -4\\ -2 & -4 & -2 & -2 & -4 & 10\end{pmatrix}\begin{pmatrix}17\\35\\25\\17\\32\\15\end{pmatrix}(mod\ 37)=\begin{pmatrix}7\\15\\15\\7\\12\\5\end{pmatrix}$$

We get Plain text=”GOOGLE”

**5.3. Proposed technique on Affine Hill Cipher:**

Prime modulus generates large key space than a composite modulus and taking q is prime number.The plaintext column vector **R**is encrypted as **S=(KR+ B)**(mod q) in which **S**is the cipher text column vector, **K** is an m×mkey matrix in $Z_q$ and The ciphertext **R**isdecrypted as **R=K(S-B)**(modq) where **K**=$I_m$-2**n**.$\mathbf{n}^T$Where $I_m$ is identity matrix, T is column vector over $Z_q$ and **n**=$\frac{B}{\|B\|}$.It should satisfyg.c.d (det **K**(mod q), q) = 1.

**5.3.1. Encryption algorithm**

Step1: Generate reflection matrix key **K** from reflection matrix key generation algorithm.

Step2:Calculate **S=(KR+B)**(mod q)

Step3: Write Cipher text

**5.3.2. Decryption algorithm**:

- Step1:In put Keys**K,B**
- Step2:Calculate **R=K(S-B)**(mod q)
- Step3:Write Plain text

**5.4. Example of Proposed technique on Affine Hill Cipher:**

Consider Plain text=”YES”

R=$\begin{pmatrix}Y\\E\\S\end{pmatrix}$is block of plain text.R=$\begin{pmatrix}25\\5\\19\end{pmatrix}$is block of plain text, Taking keys from example5.1.4

Encryption:

**S=(KR+B)**(mod 37)

$$S=\left(\begin{pmatrix}18 & 31 & 14\\31 & 14 & 19\\14 & 19 & 6\end{pmatrix}\begin{pmatrix}25\\5\\19\end{pmatrix}+\begin{pmatrix}1\\4\\3\end{pmatrix}\right)(\text{mod } 37)=\begin{pmatrix}21\\26\\7\end{pmatrix}$$

Cipher text=“UZG”

Decryption: **R=K(S-B)**(mod 37)

$$R=\begin{pmatrix}18 & 31 & 14\\ 31 & 14 & 19\\ 14 & 19 & 6\end{pmatrix}\begin{pmatrix}20\\ 22\\ 4\end{pmatrix}(\text{mod } 37)=\begin{pmatrix}25\\ 5\\ 19\end{pmatrix}$$

Which gives Plain text=”YES”

**6. Computational Cost:**

The time complexity measures the running time of the algorithm. The time complexity of the proposed technique on Hill Cipher to encrypt and to decrypt the text is O ($m^2$n) which is, which is same as the original Hill cipher. In this process $T_{Enc}$and $T_{Dec}$denote the running time for encryption and decryption of ‘m’ block of plaintext respectively.

$$T_{Enc}(\text{m}) = m^2\text{n}T_{Mul}+m^2\text{n}\,T_{Add} \cong O\,(m^2n)\,, T_{Dec}(\text{m}) = m^2\text{n}T_{Mul}+m^2\text{n}T_{Add} \cong O\,(m^2n)$$

Where $T_{Add}$ and $T_{Mul}$are the time complexities for scalar modular addition, multiplication. The time complexity measures the running time of the algorithm. The time complexity of the proposed technique on Affine Hill Cipher to encrypt and to decrypt the text is O ($m^2$n) which is, which is same as the original Affine Hill cipher. In this process $T_{Enc}$and $T_{Dec}$denote the running time for encryption and decryption of ‘m’ block of plaintext respectively.

$T_{Enc}(m) = m^2nT_{Mul}+m^2n\,T_{Add} + mnT_{AddV} \cong O\,(m^2n)\,, T_{Dec}(m) = m^2nT_{Mul}+m^2nT_{Add} + mnT_{AddV} \cong O\,(m^2n)$ Where $T_{Add}$ , $T_{Mul}$, and $T_{AddV}$are the time complexities for scalar modular addition, multiplication and addition of vector respectively.

**7. Conclusion**

This paper suggests effective approaches for generating the self-invertible matrix for Hill Cipher algorithm. These ways encompass much less computational complexity as an inverse of the matrix is not required while decrypting in Hill Cipher. The proposed method for generating Self-invertible Matrix can also be used in other algorithms where matrix inversion is required. Since the improvisation of cipher text made in this paper is relatively more secure due to the utilization of self-invertible matrix which is actually generated from the homogenous linear equation .The concept of sending the equation has made the whole procedure much protected. So, at the time of decryption, we need not find inverse of the matrix. Moreover, this method eliminates the computational complexity involved in finding the inverse of the matrix while decryption.

**References**

1. L.S. Hill, “Cryptography in an Algebraic Alphabet, “American Mathematical Monthly, Vol.36, No.6, pp.306-312, 1929

2. M.G.Vara Prasad et all "Affine hill cipher key generation matrix of order 3 by using reflects in an arbitrary line y=a x+ b" "International journal of science and technology and management Vol no:5,Issue No:8, August 2016
3. Douglas R. Stinson, Cryptography Theory and practice ,third edition (2006)by chapman & Hall/CRC Taylor &Francis Group
4. Hill Cipher Key Generation Algorithm by using Orthogonal Matrix, International Journal of Innovative Science and Modern Engineering IJISME, Volume-3 Issue-3, February 2015
5. Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, and Saroj Kumar Panigrahy. "Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm". International Journal of Security (CSS Journals). Vol. 1, Issue. (1), pp. 14-21, 2007.
6. V. U. K. Sastry, D. S. R. Murthy, and S. Durga Bhavani, A block cipher involving a key applied on both sides of the plain text," International Journal of Computer and Network Security, vol. 1, no. 1, Oct. 2009.
7. Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, and Saroj Kumar Panigrahy" Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm",1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008
8. B. Acharya, D. Jena, "Invertible, involuntary and permutation matrix generation methods for Hill cipher system", Proceedings of the 2009 International Conference on Advanced Computer Control, January22-24, 2009, Singapore, Singapore pp. 410-414
9. Abd Manaf et al."On the Affine Ciphers in Cryptography"Springer-Verlag Berlin Heidelberg 2011,pp. 185–199,
10. Y.S. Yeh, T.C. Wu, C.C. Chang, and W.C. Yang, "A New Cryptosystem Using Matrix Transformation," Proceedings of the 25th IEEE International Carnahan Conference on Security Technology, pp.131-138, Oct. 1991.
11. Koblitz, N. A Course in Number Theory and Cryptography, 2nd ed. New York: Springer- Verlag, 1994
12. Introduction to Analytic Number Theory, fifth edition. T. Apostol Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1995
13. Analysis and Design of Affine and Hill Cipher, Journal of Mathematics Research Vol. 4, No. 1; February 2012.