International Journal of Trend in Scientific Research and Development, Volume 1(4), ISSN: 2456-6470
www.ijtsrd.com

Symmetric Key Generation Algorithm in Linear Block Cipher Over LU Decomposition Method

P.Sundarayya
Department of Mathematics,
GITAM University, Visakhapatnam,
Andhra Pradesh, India

M.G.Vara Prasad
Department of Mathematics,
NSRIT, Visakhapatnam,
Andhra Pradesh, India

ABSTRACT

In symmetric key algorithm in linear block cipher to encrypt and decrypt the messages using matrix and inverse matrix. In this proposed technique generate lower and upper triangular matrices from square matrix using decomposition. In encryption process, the key is lower triangular matrix and decryption process, the key is upper triangular matrix under modulation of prime number. We illustrate the proposed technique with help of examples.

Keywords: liner block cipher, symmetric matrix key, encryption, and decryption, lower and upper triangular decomposition

1. INTRODUCTION

Cryptography is the science of making messages in secret code and having lived art. Cipher is mathematical function which is used in encryption and decryption process. Cryptography systems can be divided into two cryptosystems.

- Symmetric
- Asymmetric.

Symmetric key cryptography is classical cryptography is divided into four parts.

- The encryption algorithm
- The encryption key
- The decryption algorithm
- The decryption key

Symmetric cryptosystems use the secret keyto encrypt and decrypt message, and asymmetric cryptosystems use the public key to encrypt a message and the private key to decrypt it .Symmetric encryption is described to as conventional encryption or single key encryption. Conventional encryption can be divided into two categories.

- Classical techniques
- Modern techniques

The hallmark of Symmetric key encryption is that the cipher or key to the algorithm is shared. Linear block Cipher is one of the basic components of classical ciphers. A Liner block cipher is a method of encryption by which units of plaintext are substituted with cipher text according to a regular system; the units maybe pairs

of letters, triplets of letters, poly of letters and mixtures of the above. The receiver deciphers the text by performing an inverse function [2]. Hill cipher is a block cipher that has several advantages such as disguising

letter frequencies of the plaintext, its simplicity because of using matrix multiplication for enciphering and deciphering, its high speed, and high throughput [4].In this proposed work, Instead of matrix and inverse matrix, idea of generate the symmetric key generation can be decomposed matrix into lower and upper triangular matrices. In encryption process using lower triangular matrix and decryption process the cipher text convert into plain text using upper triangular matrix under modulation of prime number. In this proposed technique overcome of known plain text attack when the order of the key matrix known.

2. The Hill cipher

The Hill cipher algorithm takes *m* successive plaintext letters and substitute's *m* cipher text letters for them. The substitution is determined by *m* where *m* is a positive integer, the idea is to take *m* linear combinationsof the *m* alphabetic characters in one plaintext elementand produce *m* alphabetic characters in onecipher text element. Then, an $m \times m$matrix $\boldsymbol{K}$ is used asa key of the system such that $\boldsymbol{K}$ is invertible modulo *n* (Peterson, 2000; Lerma, 2005) andg.c.d((det K)mod n, n)=1. Let k_{ij}be the entryof $\boldsymbol{K}$. For the plaintext block $R=(x_1, x_2,..,x_m)$ (thenumerical equivalents of *m* letters) and a key matrix $\boldsymbol{K}$,the corresponding cipher text block $S=(y_1, y_2, \ldots, y_m)$

Encryption: The cipher text is obtained from the plaintext by means of a linear transformation.

$$S=\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{mm} \end{pmatrix} R \text{ (mod n)}$$

Decryption: The reverse process, deciphering, is computed by

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

There might be some complications with the procedure outlined above due to the fact that not all the matrices $\boldsymbol{K}$ have an inverse $\boldsymbol{K}^{-1}$ over Z_n. In fact, those matrices $\boldsymbol{K}$ with determinant 0, or with a determinant that has common factors with the modulus *n*, will be singular over Z_n, and therefore they will not be eligible as key matrices in the Hill cipher scheme (Overbey*et al*., 2005)[1]. Furthermore, due to its linear nature, the basic Hill cipher succumbs to known-plaintext attacks. Indeed, it is easy to show that an opponent able to obtain mplaintext/cipher text character pairs has a high probability of completely breaking the system, i.e., he/she can obtain the matrix $\boldsymbol{K}$ by solving the linear system of equations.

3. Cryptanalysis of known plain-text attack when m is known of Hillcipher

Despite Hill cipher being difficult to break with a cipher text-only attack, it succumbs to a known plaintext attack assuming that the opponent has determined the value of the *m* being used. Let *m*be distinct plaintext-cipher text pairs, say, $\boldsymbol{xj}=(x_{1j}, x_{2j}, \ldots, x_{mj})$ and $\boldsymbol{yj}=(y_{1j}, y_{2j}, \ldots, y_{mj})$, $1 \leq j \leq m$, such that $\boldsymbol{y}_j=e_k(\boldsymbol{x}_j)$,Define two $m \times m$ matrices $\boldsymbol{R}=(x_{ij})$ and $\boldsymbol{S}=(y_{ij})$.Whenever $\boldsymbol{K}$ is invertible in the encryption equation $\boldsymbol{S}=\boldsymbol{RK}$, the opponent can compute the unknown key of ciphering as $\boldsymbol{K}=\boldsymbol{R}^{-1}\boldsymbol{S}$ and thereby break the cipher (Barr, 2002). If $\boldsymbol{R}$ is not invertible, then it will be necessary to try other sets of *m* plaintext-cipher text pairs. When *m* is unknown, assuming that *m* is not too large, the opponent could simply try *m*=2, 3, …, until the key is found. If the guessed value of *m* was incorrect, the obtained key matrix would be not agree with further plaintext-cipher text pairs (Stinson,2002).[1]

4. The Proposed Technique

The proposed technique takes *m* successive plaintext letters and substitute's *m* cipher text letters for them. The substitution is determined by *m* where *m* is a positive integer, the idea is to take *m* linear combinationsof the *m* alphabetic characters in one plaintext elementand produce $m \times n$ constant matrix B. In this proposed technique has generation of key matrices using LU Decomposition method, i.e A=LU and g.c.d((det A)mod q, q)=1 . Now constant matrix B=AP $\Longrightarrow B = LUP$. In encryption process LC=B$\Longrightarrow$ C=L^{-1}B and decryption process UP=C$\Longrightarrow$ P=U^{-1}B where P is plain text and C is cipher text.

4.1. Generating lower and upper triangle matrices using LU decomposition method

Theorem: Every m-square matrix A can be expressed as product of two triangular matrices, one lower triangular and another upper triangular thus A=LU, where q is prime number and A∈ $Z_q^{m\times m}$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} = \begin{pmatrix} l_{11} & 0 & \cdots & 0 \\ l_{21} & l_{22} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ l_{m1} & l_{m2} & \cdots & l_{mm} \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ 0 & u_{22} & \cdots & u_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & u_{mm} \end{pmatrix}$$

Where L=$\begin{pmatrix} l_{11} & 0 & \cdots & 0 \\ l_{21} & l_{22} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ l_{m1} & l_{m2} & \cdots & l_{mm} \end{pmatrix}$ and U=$\begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ 0 & u_{22} & \cdots & u_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & u_{mm} \end{pmatrix}$

To simplify calculations we may choose $(l_{11}, l_{22}, \ldots\ldots l_{mm}) =$ (1,1, ……,1) ($Dolittle's\ method$)

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ l_{m1} & l_{m2} & \cdots & 1 \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ 0 & u_{22} & \cdots & u_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & u_{mm} \end{pmatrix}$$

WhereL=$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ l_{m1} & l_{m2} & \cdots & 1 \end{pmatrix}$ and U=$\begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ 0 & u_{22} & \cdots & u_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & u_{mm} \end{pmatrix}$

If m=2 order of matrix then A=LU becomes$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ l_{21} & 1 \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} \\ 0 & u_{22} \end{pmatrix}$

Multiplying the matrices L and U and equating corresponding elements from both sides

- $a_{11}=u_{11}$, $a_{12}=u_{12}$
- $a_{21} = l_{21}u_{11} \Rightarrow l_{21} = \frac{a_{21}}{u_{11}}$
- $a_{22} = l_{21}u_{12} + u_{22} \Rightarrow u_{22} = a_{22} - \frac{a_{21}}{u_{11}}u_{12}$

Example 4.1.1

Consider A=$\begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix} \in Z_{29}^{2\times 2}$

A=$\begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix}$ can be decomposed into L and U.A=LU⇒ $\begin{pmatrix} 4 & 2 \\ 6 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ l_{21} & 1 \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} \\ 0 & u_{22} \end{pmatrix}$

$\Rightarrow \begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} \\ l_{21}u_{11} & l_{21}u_{12} + u_{22} \end{pmatrix}$, $u_{11} = 4, u_{12} = 1, l_{21}u_{11} = 2 \Rightarrow l_{21} = \frac{1}{2}$

$l_{21}u_{12} + u_{22} = 3 \Rightarrow u_{22} = \frac{5}{2}$

L=$\begin{pmatrix} 1 & 0 \\ 15 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & 1 \end{pmatrix}$ mod 29, U=$\begin{pmatrix} 4 & 1 \\ 0 & 17 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 0 & \frac{5}{2} \end{pmatrix}$ mod 29, Therefore L, U ∈ $Z_{29}^{2\times 2}$

If m=3 order of matrix then A=LU becomes

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{pmatrix}$$

Multiplying the matrices L and U and equating corresponding elements from both sides

- $u_{11}=a_{ll}$, $u_{12}=a_{12}$, $u_{13}=a_{13}$.
- $l_{21}u_{11}=a_{21} \Rightarrow l_{21}=\frac{a_{21}}{a_{11}}$
- $l_{31}u_{11}=a_{31} \Rightarrow l_{31}=\frac{a_{31}}{a_{11}}$
- $l_{21}u_{21}+u_{22}=a_{22} \Rightarrow u_{22}=a_{22}-(\frac{a_{21}}{a_{11}})a_{12}$
- $l_{21}u_{13}+u_{23}=a_{23} \Rightarrow u_{23}=a_{23}-(\frac{a_{21}}{a_{11}})a_{13}$
- $l_{31}u_{13}+l_{32}u_{22}=a_{32} \Rightarrow l_{32}=\left(\frac{a_{32}-(\frac{a_{31}}{a_{11}})a_{12}}{a_{22}-(\frac{a_{21}}{a_{11}})a_{12}}\right)$
- $l_{31}u_{13}+l_{33}u_{23}=a_{33} \Rightarrow u_{33}=a_{33}-\left(\frac{a_{31}}{a_{11}}a_{13}\right) - \left(\frac{a_{32}-(\frac{a_{31}}{a_{11}})a_{12}}{a_{11}-(\frac{a_{21}}{a_{11}})a_{12}}\right)-\left(u_{23}-(\frac{a_{21}}{a_{11}})a_{13}\right)$

4.2. Calculation of constant matrix

Let P is block of given plain text. In that block P assigns labels fromtable -1according to given plain text. Let *B* be constant matrix and A is generator key matrix then B=AP mod q, where q is prime number.

A=$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix}$ is matrix of order m,

P=$\begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{m1} & p_{m2} & \cdots & p_{mn} \end{pmatrix}$ and

B=$\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$

$$\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{m1} & p_{m2} & \cdots & p_{mn} \end{pmatrix} (\text{mod } q)$$

4.3. Encryption

Let C be a block of cipher text and B is constant matrix then encryption can be defined as AC=B and LC=B$\Longrightarrow$ C=L^{-1}B

C=$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}$ be a block of cipher text

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ l_{m1} & l_{m2} & \cdots & 1 \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ l_{m1} & l_{m2} & \cdots & 1 \end{pmatrix}^{-1} \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

4.3.1. Encryption algorithm

Step1: Calculate B=AC (mod q)

Step2: Select Key L as square matrix order m from A=LU.

Step3: Calculate $C=L^{-1}B$

Step4:Calculate C= C (mod q)

4.4. Decryption

Let P be a block of plain text and C be a block of cipher text then$UP=C \Longrightarrow P=U^{-1}C$

$$\begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ 0 & u_{22} & \cdots & u_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & u_{mm} \end{pmatrix} \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{m1} & p_{m2} & \cdots & p_{mn} \end{pmatrix}$$

$$= \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}$$

$$\begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{m1} & p_{m2} & \cdots & p_{mn} \end{pmatrix} =$$

$$\begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ 0 & u_{22} & \cdots & u_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & u_{mm} \end{pmatrix}^{-1} \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}$$

4.4.1. Decryption algorithm

Step1: Select Key U as square matrix order m from A=LU.

Step2: Calculate $P= U^{-1} C$

Step3: Calculate P= P (mod q)

5. Example of proposed technique

Consider the plain text P='GOOGLE', $\begin{pmatrix} G & O & L \\ O & G & E \end{pmatrix}$ is block of plain text.

In the 29-letter alphabet in which A-Z have numerical equivalent 1-26,?=27,space=28

$P=\begin{pmatrix} 6 & 14 & 11 \\ 14 & 6 & 4 \end{pmatrix}$ is block of plain text

TakingFrom Example4.1.1

$A=\begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix}$ can be decomposed into L and U.

$A=LU \Rightarrow \begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 15 & 1 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 0 & 17 \end{pmatrix}$

Encryption:

B= AP mod 29

$B=\begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 6 & 14 & 11 \\ 14 & 6 & 4 \end{pmatrix}$ (mod 29)

$B=\begin{pmatrix} 9 & 4 & 19 \\ 25 & 17 & 5 \end{pmatrix}$(mod 29)

Let C= be a block of cipher text.

Encryption key $L=\begin{pmatrix} 1 & 0 \\ 15 & 1 \end{pmatrix}$

$LC=B \Longrightarrow C=L^{-1}B$ mod 29

$C=\begin{pmatrix} 1 & 0 \\ 15 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 9 & 4 & 19 \\ 25 & 17 & 5 \end{pmatrix}$ (mod 29)

$C=\begin{pmatrix} 9 & 4 & 19 \\ 14 & 15 & 10 \end{pmatrix}=\begin{pmatrix} J & E & T \\ O & P & K \end{pmatrix}$

This gives Cipher text C='JOEPTK'

Decryption:

Decryption key $U=\begin{pmatrix} 4 & 1 \\ 0 & 17 \end{pmatrix}$

$UP=C \Longrightarrow P=U^{-1}C$ mod 29

$P=\begin{pmatrix} 4 & 1 \\ 0 & 17 \end{pmatrix}^{-1}\begin{pmatrix} 9 & 4 & 19 \\ 14 & 15 & 10 \end{pmatrix}$ (mod 29)

$P=\begin{pmatrix} 6 & 14 & 11 \\ 14 & 6 & 4 \end{pmatrix}$

Which gives Plain text ='GOOGLE'

6. Cryptanalysis of proposed technique

The block cipher can be difficult to break with a cipher text only attack. In this section, we discuss Cryptanalysis of known plain-text attack. We assumed that K is key matrix is an element of $Z_q^{m\times m}$

6.1.Algorithm for known plain-text attack when m is known

Step1: Let P= (P_1,P_2,……,P_n) be a block of plain text. Where $P_i=\begin{pmatrix} p_{1i} \\ p_{2i} \\ \vdots \\ p_{mi} \end{pmatrix}$ Let C= (C_1,C_2,……,C_n) be a block of cipher text. Where $C_i=\begin{pmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{mi} \end{pmatrix}$ and select randomly pairs of plaintext and corresponding cipher text are (P_i,C_i)for i=1,2,3…….n.

Step2: The known plaintext – cipher text pairs gives us a system of equations of the form

$[C_i- C_j]=K[P_i- P_j]$ for $1\leq i\neq j\leq m$, we get general equation C=KP

Step 3: Determine $K=P^{-1}C \bmod q$

6.2. Example for cryptanalysis of proposed technique when m=2 is known

Taking from 6.Example we get plaintext blocks $P_1=\begin{pmatrix} 6 \\ 14 \end{pmatrix}$, $P_2=\begin{pmatrix} 14 \\ 6 \end{pmatrix}$,$P_3=\begin{pmatrix} 11 \\ 4 \end{pmatrix}$, cipher text blocks$C_1=\begin{pmatrix} 9 \\ 6 \end{pmatrix}$, $C_2=\begin{pmatrix} 4 \\ 15 \end{pmatrix}$,$C_3=\begin{pmatrix} 19 \\ 10 \end{pmatrix}$

then$(C_1 - C_2 \quad C_2 - C_3) = K(P_1 - P_2 \quad P_2 - P_3)$

$\begin{pmatrix} 5 & -15 \\ -9 & 5 \end{pmatrix}=K\begin{pmatrix} -8 & 3 \\ -8 & 2 \end{pmatrix} \Rightarrow K=$

$\begin{pmatrix} 5 & -15 \\ -9 & 5 \end{pmatrix}\begin{pmatrix} -8 & 3 \\ -8 & 2 \end{pmatrix}^{-1}=\begin{pmatrix} 4 & 1 \\ 0 & 17 \end{pmatrix}(\text{mod } 29)$

Conclusion

In the proposed work the symmetric key matrix of classical Hill cipher is to make changes in order to make greatest security of communication text. In this paper symmetric key generation is more secure due to the decomposition of the matrix into lower and upper triangle matrices to encrypt and decrypt the messages .The Proposed Cryptosystem to get better the plaintext attack and also to get better cipher text attack, since the lower triangle matrix is using for encryption process and upper triangle matrix is using for decryption process over residue modulo prime number

References

[1] Douglas R. Stinson,Cryptography Theory and practice ,third edition (2006)by chapman & Hall/CRC Taylor &Francis Group.

[2] Koblitz, N. A Course in Number Theory and Cryptography, 2nd ed. New York: Springer-Verlag, 1994.

[3]A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996

[4]G.R. Blakley, Twenty years of cryptography in the open literature, Security and Privacy 1999 Proceedings of the IEEE Symposium, 9-12 May1999

[5]J. Overbey, W. Traves, J. Wojdylo, On the key space of the Hill cipher. Cryptologia, 29(1), 2005, 59-72

[6]Introduction to Analytic Number Theory, fifth edition. T. Apostol .Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1995

[7]Higher engineering mathematics khanna publishers by Dr. B.S. Grewal 40th edition

[8]P.B. Bhattachary SK Jain S.R. Nagpaul First course in Linear Algebra 1983

[9] W. H.; Flannery, B. P.; Teukolsky, S. A.; and Vetterling, W. T. "LU Decomposition and Its Applications." §2.3 in Numerical Recipes in FORTRAN: The Art of Scientific Computing, 2nd ed. Cambridge, England: Cambridge University Press, pp. 34-42, 1992.

[10] Bunch, James R.; Hopcroft, John (1974), "Triangular factorization and inversion by fast matrix multiplication", Mathematics of Computation, 28 (125): 231–236

[11]Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford (2001), Introduction to Algorithms, MIT Press and McGraw-Hill,

[12]Okunev, Pavel; Johnson, Charles R. (1997), Necessary And Sufficient Conditions For Existence of the LU Factorization of an Arbitrary Matrix,

[13]ress, WH; Teukolsky, SA; Vetterling, WT; Flannery, BP (2007), "Section 2.3", Numerical Recipes: The Art of Scientific Computing (3rd ed.), New York: Cambridge University Press, ISBN 978-0-521-88068-8.

[14] SurajoAbubakarWadaInt. Journal of Engineering Research and Applications Vol. 6, Issue 2, February 2016