International Journal of Engineering, Science and Mathematics
Vol. 6 Issue 8, December 2017 (Special Issue)
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com Double-Blind
Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

CRYPTANALYSIS OF SELF -INVERTIBLE KEY GENERATION FOR AFFINE HILL CIPHER AND DIGRAPH AFFINE HILL CIPHER

P. Sundarayya[1]
M .G .Vara Prasad[2]
K.P.Satyam[3]
P.Paripurna chari[4]
Vangapandu prasad[5]

Keywords:

Self-InvertibleMatrix,
Encryptionalgorithm,
decryption algorithm,
Affine Hill cipher,
Digraph Affine Hill cipher.

Abstract:

BibhudendraAcharya in [15] proposed the concepts of Novel Methods of Generating Self-Invertible Matrix for HillCipher Algorithm. In this paper introduceDigraph Affine Hill cipheranddiscuss about cryptanalysis of Affine Hill cipher and Digraph Affine Hill cipher using Self-Invertible Matrix.

Author correspondence:

P. Sundarayya[1]
Department of Engineering Mathematics,
GITAM University
Visakhapatnam, India
M .G .Vara Prasad[2]
Department of Mathematics,
NSRIT, Visakhapatnam, India

K.P.Satyam[3]
Department of Mathematics,
NSRIT, Visakhapatnam, India

P.Paripurna chari[4]
Department of Mathematics,
NSRIT, Visakhapatnam, India

Vangapandu Prasad[5]
Assistant Professor,
Department of Mathematics,
BITS,Visakhapatnam, India,

,

1. Introduction

Today, in the information age, the need to protect communications from prying eyes is greater than ever before [5].Cryptography, the science of encryption and it plays a central role in many aspects of our daily lives like security of ATM cards, computer passwords, sending emails, e-commerce. Conventional Encryption is called symmetric encryption or single key encryption. It may be similarly divided into classes of classical techniques and modern strategies. The hallmark of traditional encryption is that the cipher or key to the set of rules is shared, i.e., regarded with the aid of the parties involved inside the secured communication exchange. Substitution cipher is one of the simple components of classical ciphers. A substitution cipher is a technique of encryption by way of which devices of plaintext are substituted with cipher text according to a regular system; the units may be single letters (the most common), pairs of letters, triplets of letters, combinations of the above, and so on. The receiver deciphers the text by using appearing an inverse substitution [3]. The units of the plaintext are retained within the identical sequence as inside the cipher text, but the devices themselves are altered. There are some of special sorts of substitution cipher. If the cipher operates on single letters, it's miles termed easy substitution cipher; a cipher that operates on large organizations of letters is named polygraphic. A monoalphabetic cipher uses constant substitution over the whole message, whereas a polyalphabetic cipher makes use of a number of substitutions at one-of-a-kind instances in the message— along with homophones, where a unit from the plaintext is mapped to considered one of several possibilities inside the cipher text. The inverse of the matrix used for encrypting the plaintext does not constantly exist. So, if the matrix is not invertible, the encrypted text can't be decrypted. In the self-invertible matrix generation method, the matrix used for the encryption is itself self-invertible. So, at the time of decryption, we want now not to find inverse of the matrix. Moreover, this technique gets rid of the computational complexity concerned in finding inverse of the matrix at the same time as decryption. BibhudendraAcharya in [5] ,generated Self-Invertible Matrix and used in Hill cipher.In this paper we discuss about cryptanalysis of Affine Hill cipher and Digraph Affine Hill cipher using Self-Invertible Matrix algorithm.

2. Preliminaries:

2.1.Self-Invertible Matrix: A square matrix A is said to be Self-Invertible Matrixif$A^{-1} = A$.

2.2.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 Q = (KP + R)(mod m) . All operations are performed over Z_m. Where R is column vector overZ_m. It should satisfy gcd (detK(mod m), m) = 1 and P is the plain text, Q is the cipher text.

Encryption:

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

Decryption:

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

3. A General method of generating an even orderself-invertible matrix under modulation of a prime number:

Let $K=\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix}$ be a matrix of order n and p be a prime number.

Then $K=\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix}$ be an $n \times n$ self $-$ invertible matrix partitioned into

$K=\begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix}$ where n is even and K_{11}, K_{12}, K_{21} and K_{22} are matrices of order $\frac{n}{2}\times\frac{n}{2}$ each.

Construction of *an even* self $-$ invertible matrix

- Select any arbitrary $\frac{n}{2}\times\frac{n}{2}$ matrix K_{22}
- Obtain $K_{11}=-K_{22}(\text{ mod p})$
- If take $K_{12}=c(I-K_{11})(\text{mod p})$ then $K_{21}=\frac{(I+K_{11})}{c}(\text{mod p})$ where c is a scalar constant and I is the identity matrix.
- Form the matrix completely

3.1.Example:

Let p=37,let n=2,let $K_{22}=4$,let c=2

$K_{11}=-K_{22}(\text{ mod p}) \Rightarrow K_{11}=-4(\text{mod } 37) \Rightarrow K_{11}=33$

$K_{12}=2(I-K_{11})(\text{mod p}) \Rightarrow K_{12}=2(1-33)(\text{mod } 37) \Rightarrow K_{12}=10$

$K_{21}=\frac{(I+K_{11})}{c}(\text{mod p}) \Rightarrow K_{21}=\frac{(1+33)}{2}(\text{mod } 37) \Rightarrow K_{21}=17(\text{mod } 37)$

There fore $K=\begin{pmatrix} 33 & 10 \\ 17 & 4 \end{pmatrix}(\text{mod } 37)$ is an even order self-invertible matrix.

3.2.Example:

Let p=37,let n=2,let $K_{22}=4$,let c=1

$K_{11}=-K_{22}(\text{ mod } p^2) \Rightarrow K_{11}=-4(\text{mod } 37^2) \Rightarrow K_{11}=1365$

$K_{12}=(I-K_{11})(\text{mod } p^2) \Rightarrow K_{12}=(1-1365)(\text{mod } 37^2) \Rightarrow K_{12}=5$

$K_{21}=\frac{(I+K_{11})}{c}(\text{mod } p^2) \Rightarrow K_{21}=(1+1365)(\text{mod } 37^2) \Rightarrow K_{21}=1366(\text{mod } 37^2)$

There fore $K=\begin{pmatrix} 1365 & 5 \\ 1366 & 4 \end{pmatrix}(\text{mod } 37^2)$ is an even order self-invertible matrix.

3.3.Example:

Let p=37,let n=4,let $K_{22}=\begin{pmatrix} 10 & 2 \\ 3 & 4 \end{pmatrix}$,let c=1

$K_{11} = -K_{22}(\text{mod p}) \Rightarrow K_{11} = -\begin{pmatrix}10 & 2\\ 3 & 4\end{pmatrix}(\text{mod } 37) \Rightarrow K_{11} = \begin{pmatrix}27 & 35\\ 34 & 33\end{pmatrix}(\text{mod } 37)$

$K_{12} = c(I - K_{11})(\text{mod p}) \Rightarrow K_{12} = (I - K_{11})(\text{mod } 37) \Rightarrow K_{12} = \left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - \begin{pmatrix}27 & 35\\ 34 & 33\end{pmatrix}\right)(\text{mod } 37) = \begin{pmatrix}11 & 2\\ 3 & 5\end{pmatrix}$

$K_{21} = \frac{(I + K_{11})}{c}(\text{mod p}) \Rightarrow K_{21} = \begin{pmatrix}28 & 35\\ 34 & 34\end{pmatrix}$

There fore $K = \begin{pmatrix}27 & 35 & 11 & 2\\ 34 & 33 & 3 & 5\\ 28 & 35 & 10 & 2\\ 34 & 34 & 3 & 4\end{pmatrix}(\text{mod } 37)$ is an even order self-invertible matrix.

4.An even order self-invertible matrix on Affine Hill Cipher:

Prime modulus generates large key space than a composite modulus and taking q is prime number. The plaintext column vector **P**is encrypted as **Q= (KP+ R)**(mod q) in which **Q**is the cipher text column vector, **K** is an even order$m \times m$ key matrix in Z_q and The cipher text **Q**is decrypted as
P= K(Q-R) (mod q) where R=$\mathbf{K}_i(1 \leq i \leq m)$ is one of the column vector K over $Z_q$andIt should satisfy g.c.d (det**K**(mod q), q) = 1.If the length of the plain text is odd then add space letter to given plain text so that the length of the plain text is even.

4.1. Encryption algorithm

- Step1: Generate even order self –invertible matrix key **K**.
- Step2: Calculate **Q= (KP+R)**(mod q)
- Step3: Write Cipher text

4.2. Decryption algorithm:

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

4.3.An example of even order self-invertible matrix on Affine Hill Cipher:

In the 37-letter alphabet in which A-Z have numerical equivalent 0-25,0-9 have numerical equivalent 26-35,space=36. And q=37.
Now consider plain text “YK17”

P=$\begin{pmatrix}Y\\ K\\ 1\\ 17\end{pmatrix}$ is block of plain text. P=$\begin{pmatrix}24\\ 10\\ 27\\ 33\end{pmatrix}$ is block of plain text.

Taking keys from example 3.2, we get K = $\begin{pmatrix}27 & 35 & 11 & 2\\ 34 & 33 & 3 & 5\\ 28 & 35 & 10 & 2\\ 34 & 34 & 3 & 4\end{pmatrix}$ and R=$\begin{pmatrix}27\\ 34\\ 28\\ 34\end{pmatrix}$

Encryption:
Q= (KP+R)(mod 37)

Q=$\left(\begin{pmatrix}27 & 35 & 11 & 2\\ 34 & 33 & 3 & 5\\ 28 & 35 & 10 & 2\\ 34 & 34 & 3 & 4\end{pmatrix}\begin{pmatrix}24\\ 10\\ 27\\ 33\end{pmatrix} + \begin{pmatrix}27\\ 34\\ 28\\ 34\end{pmatrix}\right)(\text{mod } 37)$

Q=$\begin{pmatrix}19\\ 20\\ 17\\ 34\end{pmatrix}(\text{mod } 37)$

Cipher text=“TUR8”

Decryption:**P=K(Q-R)** (mod 37)

$R=\begin{pmatrix}27 & 35 & 11 & 2\\ 34 & 33 & 3 & 5\\ 28 & 35 & 10 & 2\\ 34 & 34 & 3 & 4\end{pmatrix}\begin{pmatrix}19\\20\\17\\34\end{pmatrix}(\text{mod } 37)=\begin{pmatrix}24\\10\\27\\33\end{pmatrix}$

Which gives original plain text is "YK17"

Now consider another plain text "YEAR2017"

$P=\begin{pmatrix}Y & A & 2 & 1\\ E & R & 0 & 7\end{pmatrix}$ is block of plain text. $P=\begin{pmatrix}24 & 0 & 28 & 27\\ 4 & 17 & 26 & 33\end{pmatrix}$ is block of plain text.

Taking keys from example 3.1, we get $K=\begin{pmatrix}33 & 10\\ 17 & 4\end{pmatrix}$, $R=\begin{pmatrix}10\\4\end{pmatrix}$

Encryption:**Q= (KP+R)**(mod 37)

$$\mathbf{Q_1}=\left(\begin{pmatrix}33 & 10\\ 17 & 4\end{pmatrix}\begin{pmatrix}24\\4\end{pmatrix}+\begin{pmatrix}10\\4\end{pmatrix}\right)(\text{mod } 37)=\begin{pmatrix}28\\21\end{pmatrix}$$
$$\mathbf{Q_2}=\left(\begin{pmatrix}33 & 10\\ 17 & 4\end{pmatrix}\begin{pmatrix}0\\17\end{pmatrix}+\begin{pmatrix}10\\4\end{pmatrix}\right)(\text{mod } 37)=\begin{pmatrix}32\\35\end{pmatrix}$$
$$\mathbf{Q_3}=\left(\begin{pmatrix}33 & 10\\ 17 & 4\end{pmatrix}\begin{pmatrix}28\\26\end{pmatrix}+\begin{pmatrix}10\\4\end{pmatrix}\right)(\text{mod } 37)=\begin{pmatrix}10\\29\end{pmatrix}$$
$$\mathbf{Q_4}=\left(\begin{pmatrix}33 & 10\\ 17 & 4\end{pmatrix}\begin{pmatrix}27\\33\end{pmatrix}+\begin{pmatrix}10\\4\end{pmatrix}\right)(\text{mod } 37)=\begin{pmatrix}10\\3\end{pmatrix}$$

Cipher text $Q=(\mathbf{Q_2},\mathbf{Q_2},\mathbf{Q_3},\mathbf{Q_4})$="2V69K3KD"

Decryption:**P=K(Q-R)** (mod 37)

$$\mathbf{P_1}=\begin{pmatrix}33 & 10\\ 17 & 4\end{pmatrix}\begin{pmatrix}28\\21\end{pmatrix}(mod\ 37)=\begin{pmatrix}24\\4\end{pmatrix}$$
$$\mathbf{P_2}=\begin{pmatrix}33 & 10\\ 17 & 4\end{pmatrix}\begin{pmatrix}22\\31\end{pmatrix}(mod\ 37)=\begin{pmatrix}0\\17\end{pmatrix}$$
$$\mathbf{P_3}=\begin{pmatrix}33 & 10\\ 17 & 4\end{pmatrix}\begin{pmatrix}0\\25\end{pmatrix}(mod\ 37)=\begin{pmatrix}28\\26\end{pmatrix}$$
$$\mathbf{P_4}=\begin{pmatrix}33 & 10\\ 17 & 4\end{pmatrix}\begin{pmatrix}0\\36\end{pmatrix}(mod\ 37)=\begin{pmatrix}27\\33\end{pmatrix}$$

This gives original plain text $P=(\mathbf{P_1},\mathbf{P_2},\mathbf{P_3},\mathbf{P_4})$ ="YEAR2017"

5. Cryptanalysis of known plaintext attack when m is known on Affine Hill cipher:

The Affine Hill Cipher, the opponent has to know the values of the size m of the plaintext block size n of the cipher text block and the constant vector b to determine the matrix of the transformation even for a known plaintext attack. Let us assume that the opponent has determined the value of the *m* being used. Let *m*be distinct plaintext-cipher text pairs, say, $\boldsymbol{x}j=(x_{1j}, x_{2j}, \ldots, x_{mj})$ and $\boldsymbol{y}j=(y_{1j}, y_{2j}, \ldots, y_{mj})$, $1\leq j\leq m$, such that $\boldsymbol{y}_j=e\boldsymbol{k}(\boldsymbol{x}_j)$+b,Define$m\times m$matrices$\boldsymbol{P}=(x_{ij})$ and $\boldsymbol{Q}=(y_{ij})$.Whenever ***K***is invertible in the encryption equation $\boldsymbol{Q=KP+R}$, one has to choose a differentcontinuous pair of plaintext-cipher text pairs.

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

Step1: Let $P=(P_1,P_2,\ldots\ldots,P_n)$ be a block of plain text. Where $P_i=\begin{pmatrix}p_{1i}\\p_{2i}\\\vdots\\p_{mi}\end{pmatrix}$.

Let Q= ($C_1, C_2, \ldots\ldots, C_n$) be ablock of cipher text. Where $C_i = \begin{pmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{mi} \end{pmatrix}$

Select continuous pairs of plaintext andtheir 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 $K=P^{-1}C \pmod q$

Step 4:Determine R, substitute K,P, C in C=(KP+R)(mod q)

5.2. Example for cryptanalysis when m=2 is known

Taking from Example 4.3, we get plaintext blocks are $P_1=\begin{pmatrix}24\\4\end{pmatrix}$, $P_2=\begin{pmatrix}0\\17\end{pmatrix}$,$P_3=\begin{pmatrix}28\\26\end{pmatrix}$, corresponding cipher text blocks are$C_1=\begin{pmatrix}28\\21\end{pmatrix}$, $C_2=\begin{pmatrix}32\\35\end{pmatrix}$,$C_3=\begin{pmatrix}10\\29\end{pmatrix}$

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

$$\begin{pmatrix}33 & 22\\23 & 6\end{pmatrix} = K\begin{pmatrix}24 & 9\\24 & 28\end{pmatrix} \Rightarrow K = \begin{pmatrix}33 & 22\\23 & 6\end{pmatrix}\begin{pmatrix}24 & 9\\24 & 28\end{pmatrix}^{-1} = \begin{pmatrix}33 & 10\\17 & 4\end{pmatrix}$$

$Q=(KP+R) \Rightarrow R=Q-KP=\begin{pmatrix}28\\21\end{pmatrix} - \begin{pmatrix}18\\17\end{pmatrix} = \begin{pmatrix}10\\4\end{pmatrix}$

To overcome this we make use of Digraph Affine Hill Cipher

6. Digraph Affine Hill Cipher:

The Digraph 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.The plaintext column vector **P**is encrypted as **Q=** (P**K+ R)**(mod q^2) in which **Q**is the cipher text column vector, **K** is an $m \times m$ key matrix in Z_{q^2} and The cipher text **Q**is decrypted as**P**= $(\mathbf{Q} - \mathbf{R})\boldsymbol{K^{-1}} \pmod{q^2}$ where R=$\mathbf{K}_i (1 \leq i \leq m)$ is one of the column vector K over Z_{q^2} andIt should satisfy g.c.d $(\det\mathbf{K} \pmod q, q) = 1$.Where q is prime number .Let n be an even length plaintext. If n is not even length of plain text add space letter then n+1 will be even.Letplain text $\mathbf{P}=(P_1, P_2, P_3, \ldots \ldots P_{n/2})$ andcipher text $\mathbf{Q}=(Q_1, Q_2, Q_3, \ldots \ldots Q_{n/2})$. In Digraph Affine cipher, plaintext and cipher text messages are 2-letter blocks, called digraphs. i.e plaintext is combined into 2-letter segments. If the entire plaintext has odd number of letters, then in order to obtain a whole number of digraphs add an extra letter(space) at the end.

$P_{\frac{i}{2}+1} = (x_{i+1}q + x_{i+2}) \pmod{q^2}$ (1)

where i=0,2,4,6…….n-2, $x_i$is the numerical equivalent of the i^{th} letter of plaintext in the digraph Cipher text is split into 2-letter segments.

$Q_{\frac{i}{2}+1} = (y_{i+1}q + y_{i+2}) \pmod{q^2}$ (2)

where i=0,2,4,6…….n-2, $y_i$is the numerical equivalent of the i^{th}letter of cipher text in the digraph. In decryption process cipher text is combined into 2-letter segments using (2),after decryption plaintext is split into 2-letter segments using (1)

Encryption:

combined into $2-$ letter segments$P_{\frac{i}{2}+1} = (x_{i+1}q + x_{i+2}) \pmod{q^2}$where i=0,2,4,6…….n-2

Q_j=(P$_j$ $\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix}$ + R) (modq^2)where j=1,2,…$\frac{n}{2}$

split into 2-letter segments$Q_{\frac{i}{2}+1} = (y_{i+1}q + y_{i+2})$)(modq^2)where i=0,2,4,6…….n-2

Decryption:

combine into 2 − letter segments$Q_{\frac{i}{2}+1} = (y_{i+1}q + y_{i+2}))$(mod$q^2$)where i=0,2,4,6…….n-2

P_j=$(Q_j - R)\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix}^{-1}$ (modq^2) where j=1,2,…$\frac{n}{2}$

split into 2-letter segments $P_{\frac{i}{2}+1} = (x_{i+1}q + x_{i+2})$)(modq^2)where i=0,2,4,6…….n-2

7.An even order self-invertible matrix on Digraph Affine Hill Cipher:

The plaintext column vector **P**is encrypted as **Q**= (**K**P+ **R)**(mod q^2)) in which **Q**is the cipher text column vector, **K** is an even order$m\times m$ key matrix in Zq^2) and The cipher text **Q**is decrypted as **P**= **K(Q-R)** (mod q^2)) where R=**K**$_i$(1≤ $i \leq$ m) is one of the row vector K over Zq^2) andIt should satisfy g.c.d (det**K**(mod q), q) = 1 .Let plain text **P**=($P_1, P_2, P_3, \ldots \ldots P_{n/2}$) andcipher text **Q**=($Q_1, Q_2, Q_3, \ldots \ldots Q_{n/2}$).

Encryption:

Theplaintext is combining into 2-letter segments

iecombine into 2 − letter segments$P_{\frac{i}{2}+1} = (x_{i+1}q + x_{i+2})$)(modq^2)where i=0,2,4,6…….n-2

$Q = (PK + R)\ (\text{mod}\ q^2)$

split into 2-letter segments$Q_{\frac{i}{2}+1} = (y_{i+1}q + y_{i+2})$)(modq^2)where i=0,2,4,6…….n-2

It can be written as $Q_{\frac{i}{2}+1} = (y_{i+1}, y_{i+2})$where i=0,2,4,6…….n-2

Decryption:

combine into 2 − letter segments$Q_{\frac{i}{2}+1} = (y_{i+1}q + y_{i+2}))$(mod$q^2$)where i=0,2,4,6…….n-2

$P = (Q - R)K(\text{mod}q^2)$

split into 2-letter segments $P_{\frac{i}{2}+1} = (x_{i+1}q + x_{i+2})$)(modq^2)where i=0,2,4,6…….n-2

It can be written as $P_{\frac{i}{2}+1} = (x_{i+1}, x_{i+2})$where i=0,2,4,6…….n-2.

7.1.An example of even order self-invertible matrix on Digraph Affine Hill Cipher:

In the 37-letter alphabet in which A-Z have numerical equivalent 0-25,0-9 have numerical equivalent 26-35,space=36. And q=37.

Plain text=YEAR2017, Length of the plain text n=8,P=(P_1, P_2, P_3, P_4) where P_1=(24 ,4), P_2=(0 ,17),P_3=(28 ,26),P_4=(27 ,33)

Taking keys from example 3.2, we getK = $\begin{pmatrix} 1365 & 5 \\ 1366 & 4 \end{pmatrix}$, R=(1365 5)

Encryption:

combine into $2-$ letter segments$P_{\frac{i}{2}+1} = (x_{i+1}q + x_{i+2}))(\mathrm{mod}q^2)$where i=0,2,4,6

For i=0,$P_1 = (37x_1 + x_2)\ )(\mathrm{mod}37^2) \Rightarrow P_1 = ((24)(37) + 4)\ )(\mathrm{mod}37^2) = 892(\mathrm{mod}37^2)$
For i=2,$P_2 = (37x_3 + x_4)\ )(\mathrm{mod}37^2) \Rightarrow P_2 = ((0)(37) + 17)\ )(\mathrm{mod}37^2) = 17(\mathrm{mod}37^2)$
For i=4,$P_3 = (37x_5 + x_6)\ )(\mathrm{mod}37^2) \Rightarrow P_3 = ((28)(37) + 26)\ )(\mathrm{mod}37^2) = 1062(\mathrm{mod}37^2)$
For i=6,$P_1 = (37x_7 + x_8)\ )(\mathrm{mod}37^2) \Rightarrow P_4 = ((27)(37) + 33)\ )(\mathrm{mod}37^2) = 1032(\mathrm{mod}37^2)$
Aftercombine into $2-$ letter segments,$P_1 = 892, P_2 = 17, P_3 = 1062, P_4 = 1032$

$Q = (PK + R)\ (\mathrm{mod}\ 37^2)$

$$\boldsymbol{Q} = \left((892\ \ 17)\begin{pmatrix}1365 & 5\\ 1366 & 4\end{pmatrix} + (1365\ \ 5)\right)(\mathrm{mod}\ 37^2) = (484\ \ 426)$$

$$\boldsymbol{Q} = \left((1062\ \ 1032)\begin{pmatrix}1365 & 5\\ 1366 & 4\end{pmatrix} + (1365\ \ 5)\right)(\mathrm{mod}\ 37^2) = (1354\ 1229)$$

Split into 2-letter segments$Q_{\frac{i}{2}+1} = (y_{i+1}q + y_{i+2})\ )(\mathrm{mod}q^2)$where i=0,2,4,6

For i=0,$Q_1 = 484 = (y_1 37 + y_2)\ )(\mathrm{mod}37^2) \Rightarrow Q_1 = (13(37) + 3)\ )(\mathrm{mod}37^2) \Rightarrow Q_1 = (13, 3)$
For i=2,$Q_2 = 426 = (y_3 37 + y_4)\ )(\mathrm{mod}37^2) \Rightarrow Q_2 = (11(37) + 19)\ )(\mathrm{mod}37^2) \Rightarrow Q_2 = (11, 19)$
For i=4,$Q_3 = 1354 = (y_5 37 + y_6)\ )(\mathrm{mod}37^2) \Rightarrow Q_3 = (36(37) + 22)\ )(\mathrm{mod}37^2) \Rightarrow Q_3 = (36, 22)$
For i=6,$Q_4 = 1229 = (y_7 37 + y_8)\ )(\mathrm{mod}37^2) \Rightarrow Q_4 = (33(37) + 8)\ )(\mathrm{mod}37^2) \Rightarrow Q_4 = (33, 8)$.

∴Cipher text $Q = (Q_1, Q_2, Q_3, Q_4)$ ="NDLT W7I"

Decryption:

combine into $2-$ letter segments$Q_{\frac{i}{2}+1} = (y_{i+1}q + y_{i+2}))(\mathrm{mod}q^2)$where i=0,2,4,6

For i=0,$Q_1 = (y_1 37 + y_2)\ )(\mathrm{mod}37^2) \Rightarrow Q_1 = (13(37) + 3)\ )(\mathrm{mod}37^2) = 484(\mathrm{mod}37^2)$
For i=2,$Q_2 = (y_3 37 + y_4)\ )(\mathrm{mod}37^2) \Rightarrow Q_2 = (11(37) + 19)\ )(\mathrm{mod}37^2) = 426(\mathrm{mod}37^2)$
For i=4,$Q_3 = (y_5 37 + y_6)\ )(\mathrm{mod}37^2) \Rightarrow Q_3 = (36(37) + 22)\ )(\mathrm{mod}37^2) = 1354(\mathrm{mod}\ 37^2)$
For i=6,$Q_4 = (y_7 37 + y_8)\ )(\mathrm{mod}37^2) \Rightarrow Q_4 = (33(37) + 8)\ )(\mathrm{mod}37^2) = 1229(\mathrm{mod}37^2)$
After combine into $2-$ letter segments,$Q_1 = 484, Q_2 = 426, Q_3 = 1354, Q_4 = 1229$

$P = (Q - R)K(\mathrm{mod}37^2)$

$$P = \left((488\ \ 430)\begin{pmatrix}1365 & 5\\ 1366 & 4\end{pmatrix}\right)(\mathrm{mod}37^2) = (893\quad 17)$$

$$P = \left((8701224)\begin{pmatrix}1365 & 5\\ 1366 & 4\end{pmatrix}\right)(\mathrm{mod}\ 37^2) = (10621032)$$

Split into $2-$ letter segments$P_{\frac{i}{2}+1} = (x_{i+1}q + x_{i+2}))(\mathrm{mod}q^2)$where i=0,2,4,6

For i=0,$P_1 = 892 \Rightarrow P_1 = \big((24)(37) + 4\big)(\mathrm{mod}37^2) \Rightarrow P_1 = (24, 4)$
For i=2,$P_2 = 17 \Rightarrow P_2 = ((0)(37) + 17)\ )(\mathrm{mod}37^2) \Rightarrow P_2 = (0,17)$
For i=4,$P_3 = 1062 \Rightarrow P_3 = ((28)(37) + 26)\ )(\mathrm{mod}37^2 \Rightarrow P_3 = (28,26)$
For i=6,$P_4 = 1032 \Rightarrow P_4 = ((27)(37) + 33)\ )(\mathrm{mod}37^2) \Rightarrow P_4 = (27,33)$

It gives original plaintext ="YEAR2017"

8. Cryptanalysis of known plaintext attack when m is known on Digraph Affine Hill cipher:

The Digraph Affine Hill Cipher, the opponent has to know the values of the size m of the plaintext block size n of the cipher text block and the constant vector b to determine the matrix of the transformation even for a known plaintext attack. Let us assume that the opponent has determined the value of the *m* being used. Let *m*be distinct plaintext-cipher text pairs, say, $\boldsymbol{x}j=(x_{1j}, x_{2j}, \ldots, x_{mj})$ and $\boldsymbol{y}j=(y_{1j}, y_{2j}, \ldots, y_{mj})$, $1 \le j \le m$, such that $\boldsymbol{y}_j = e\boldsymbol{k}(\boldsymbol{x}_j)+b$,Define$m \times m$matrices$\boldsymbol{P}=(x_{ij})$ and $\boldsymbol{Q}=(y_{ij})$.Whenever $\boldsymbol{K}$is invertible in the

encryption equation ***Q=PK+R***, one has to choose a different continuous pair of plaintext-cipher text pairs.

8.1. Example for cryptanalysis when m=2 is known

Taking from Example 7.1, we get plaintext blocks are $P_1=(24,4)$, $P_2=(0,17)$,$P_3=(28,26)$, $P_4=(27,33)$, corresponding cipher text blocks are$Q_1=(13,3)$, $Q_2=(11,19)$, $Q_3=(36,22)$, $Q_4=(33,8)$.

By using 5.1. Algorithm for known plain-text attack when m is knownthen

$$\begin{pmatrix} Q_1-Q_2 \\ Q_2-Q_3 \end{pmatrix} = \begin{pmatrix} P_1-P_2 \\ P_2-P_3 \end{pmatrix} K$$

$$\begin{pmatrix} 2 & 21 \\ 12 & 34 \end{pmatrix} = K \begin{pmatrix} 24 & 24 \\ 9 & 28 \end{pmatrix} \Rightarrow K = \begin{pmatrix} 24 & 24 \\ 9 & 28 \end{pmatrix}^{-1} \begin{pmatrix} 33 & 22 \\ 23 & 6 \end{pmatrix} (mod\ 37) = \begin{pmatrix} 30 & 18 \\ 4 & 6 \end{pmatrix}$$

But In example 7.1 we used the key K=$\begin{pmatrix} 1365 & 5 \\ 1366 & 4 \end{pmatrix}$

So, By using this method we avoid known plain text attack when m is known.

9. CONCLUSION

In this proposed system introduce Digraph Affine Hill cipher which is more secure than Affine Hill Cipher.These strategies envelop less computational complexity as inverse of the matrix isnot required while decrypting in Affine Hill Cipher and Digraph Affine Hill cipher.Digraph Affine Hill cipher avoids known plain text attack.

.

REFERENCES:

[1]L. S. Hill, "Cryptography in an algebraic alphabet,"American Mathematical Monthly, vol. 36,no. 6, pp. 306–312, 1929.

[2]W. Stallings,Cryptography and Network Security: Principles and Practice, 5th ed., Boston:Prentice Hall, 2011.

[3]V. U. K. Sastry, D. S. R. Murthy, and S. DurgaBhavani, "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, pp. 27–30, Oct. 2009.

[4]L. Keliher, "Cryptanalysis of a modified Hill Cipher,"International Journal of Computer andNetwork Security, vol. 2, no. 7, pp. 122–126, Jul. 2010.

[5]S. Saeedinia, "How to make the Hill Cipher secure,"Cryptologia, vol. 24, no. 4, pp.353–360, Oct. 2000.

[6]C. H. Lin, C. Y. Lee, and C. Y. Lee, "Comments on Saeednia's improved scheme for the Hill Cipher,"Journal of the Chinese Institute of Engineers, vol. 27, no. 5, pp. 743–746, 2004.

[7]I. A. Ismail, M. Amin, and H. Diab, "How to repair the Hill Cipher,"
Journal of Zhejiang University SCIENCE A, vol. 7, no. 12, pp. 2022–2030, 2006.

[8]C. Li, D. Zhang, and G. Chen, "Cryptanalysis of an image encryption scheme based on the

Hill Cipher,"Journal of Zhejiang University SCIENCE A, vol. 9, no. 8, pp. 1118–1123, 2008.

[9]M. Toorani and A. Falahati, "A secure variant of the Hill Cipher,"Proc. IEEE Symposium on Computers and Communications (ISCC'09), Sousse, Tunisia, Jul. 2009, pp 313–316.

[10]M. Toorani and A. Falahati, "A secure cryptosystem based on affine transformation," Journalof Security and Communication Networks, vol. 4, no. 2, pp. 207–215, Feb. 2011.

[11]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.

[12]IndivarGupta,Jasbir sing and Roopikachaudhary, "Cryptanalysis of an Extension of the Hill Cipher" Crytologia, 31:246–253,2007.

[13]M.G.VaraPrasad , P.sundarayya,"Generalized self-invertible key generation algorithm by using Reflection matrix in Hill cipher and Affine Hill cipher" IJPT , Vol. 8, Issue No.4 Dec-2016

[14]D. R. Stinson, Cryptography: Theory and Practice, 3rd ed., Boca Raton: Chapman &Hall/CRC, 2006.

[15**]**BibhudendraAcharya, GirijaSankarRath, Sarat Kumar Patra, Saroj Kumar Panigrahy. "Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm", International Journal of Security, Vol 1, Issue 1, 2007.

[16] P.sundarayya, M.G.Vara Prasad, "Some technique algorithms of extension of affine cipher cryptosystem using residue modulo prime number" open journal of applied & theoretical mathematics (ojatm)vol. 2, no. 4, Dec- 2016.