An Asymmetric Cryptosystem of Skewed Affine Cipher Over Elliptic Curves with Block Matrix

ECS Transactions, 107 (1) 15903-15914 (2022)
10.1149/10701.15903ecst ©The Electrochemical Society

An Asymmetric Cryptosystem of Skewed Affine Cipher over Elliptic Curves with Block Matrix

Jayanti Sravani[a], K Chittibabu[a], and Prof. A Chandra Sekhar[a]

[a] Department of Mathematics, GITAM, Visakhapatnam 530045, Andhra Pradesh, India

The retaining of confidentiality in data transmission with user authentication has become eminent for easy and secure communication. This is achieved by using the art of cryptology at its best. Various ciphers are developed balancing time, memory, and security. In particular, the invertible property is the basic requirement in constructing a secure cryptosystem. In this paper, an invertible Block matrix is constructed over Fibonacci sequences. The sender and the recipient can derive the block matrix through the key exchanged over a secure channel for encryption and decryption. Also, an asymmetric cryptosystem is designed based on the skewed Affine cipher, which uses a bijective map over points on an Elliptic curve. The developed cryptosystem is resistant to cryptanalytic attacks.

Introduction

Classical ciphers and modern cryptography are evolved by using the concepts of mathematics. The historical cipher, such as Caesar cipher, used residue modulo to perform encryption. Hill Cipher uses the concept of matrix algebra and Number theory. The process of coding information into a disguised format and retrieving it by the authenticated user and trials made by the attacker to hack the data is an endless cycle. But providing an optimal cipher that can adapt well in terms of memory management, runtime and security is an appreciably welcoming task.

Thus there is a need for efficient mathematical models to design a secure and efficient cryptosystem. There are advancements in this field with a variety of combinations of ciphers which include Elliptic curves, concepts of linear algebra, pre-defined functions in mathematica(11)(12), and many more(7)(13)(14)(15).

In (1), an Augmented hill Cipher is proposed, which is resistant to all kinds of attacks and has greater key space with the same complexity as other versions of Hill cipher. In (3), Elliptic curve Cryptography and Hill cipher are combined to encrypt images, and detailed security analysis for the proposed approach is explained. In (5), ECC and finite fields have served as the basis for the proposed method, which is resistant to cryptanalytic attacks. In (6), the analysis and design of the Affine and Hill ciphers are discussed. In (8), a detailed study with proof is listed regarding the determinants of Block matrices which help in understanding the invertible nature of the Block matrices. In (9), an encryption algorithm is proposed using the Fibonacci Q_λ matrix, which is invertible, and the strength of the developed algorithm is discussed mathematically. In (10), a secure

text-based cryptosystem is designed with the help of the concepts of ECC and hill cipher, which requires a shorter key size.

Defining a function f(x) so that it is infeasible to compute $f^{-1}(x)$ by the intruder is the basis for designing a cryptosystem. In this paper, we developed a mathematical model for constructing a block matrix with a Fibonacci matrix and a bijective map from the character set to the points on an Elliptic curve to encrypt and decrypt blocks of 8 characters at a time.

The proposed method is derived from the concepts discussed below in brief(2)(4)(16):

Cryptography can be divided into three parts depending upon the usage of keys: Symmetric cryptography, Asymmetric cryptography, and hash functions. Symmetric cryptography uses a private key in the cryptosystem, and Asymmetric cryptography uses a set of public and private keys in the cryptosystem. In contrast, Hash functions don't use any keys for performing encryption and decryption.

Elliptic curve

An elliptic curve over real numbers is

$$y^2 = x^3 + ax + b \quad [1]$$

If $4a^3 + 27b^2 \neq 0$, then the curve is a non-singular Elliptic curve. Else, it is a singular Elliptic curve.

The points on an EC over modulo a prime p>3

$$E_p(a, b): y^2 = x^3 + ax + b(\text{mod } p) \quad [2]$$

form a cyclic group with respect to point addition on Elliptic curves where each point is a generator point when the order of the group is prime or the product of distinct primes.

Skewed Affine cipher

A cipher that looks like Affine but is not entirely Affine is a Skewed Affine cipher.

Fibonacci sequence

A sequence of the form $< f_n >$ where $f_n = f_{n-1} + f_{n-2}$ with the initial condition $f_0 = 0, f_1 = 1$ is called a Fibonacci sequence.

Fibonacci matrix

A matrix generated using numbers of the Fibonacci sequence of the form $F = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ is called Fibonacci matrix where F_n= nth Fibonacci number. The specialty of this matrix lies in the fact that it is invertible.

Block matrix

A matrix of the form $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ where A, B, C, and D are individual matrices of smaller order compatible with forming M.

The determinant of a block matrix M,

$$\det(M) = \det(A - BD^{-1}C) \,.\, \det(D) \quad [3]$$

In a special case where $M = \begin{bmatrix} A & B \\ O & D \end{bmatrix}$ where O = zero matrix, the determinant of M,

$$\det(M) = \det(A) \,.\, \det(D) \quad [4]$$

Hence, we can conclude that M is invertible provided that A and D are invertible (8)(17).

Proposed Method

Let G(x,y) be a point on the chosen Elliptic curve(EC) $E_p(q, r)$. Choose G and EC so that the order of G in EC is greater than the order of the character set. Let $'Y'$ be any random matrix of order 4 * 4. Then the Public key is (G, Y), and the Elliptic curve is shared privately.

Define a bijective map from the points on the Elliptic curve to English alphabets from 'A' to 'Z' as 1G, 2G,…, 26G. The character space is assigned the value 27G.
Generation of the key matrix:

Let $F = \begin{bmatrix} F_{r+1} & F_r \\ F_r & F_{r-1} \end{bmatrix}$ be a non-singular Fibonacci matrix.

Construct $F' = \begin{bmatrix} F & I \\ I & F \end{bmatrix}$ where I_{2*2} is an identity matrix.

Then construct the block matrix $A = \begin{bmatrix} F' & Y \\ O & F' \end{bmatrix}$ where O_{4*4} is a zero matrix.

Also, construct $B = \begin{bmatrix} F' \\ F' \\ F' \\ F' \end{bmatrix}$, which is an 8*2 matrix.

C++ code to generate the key matrices A and B

```
#include<iostream>
#include<cmath>
using namespace std;
int F(int fn)
{
    int t1=0, t2=1, nt;
    if(fn==0 || fn==1)
        return fn;
    else
        nt=t1+t2;
    for(int i=2;i<=fn;i++)
    {
        t1=t2;
        t2=nt;
        nt=t1+t2;
    }
    return t2;
}
main()
{
    int r,A[8][8], B[8][2], Y[4][4];
    cout<<"input r:";
    cin>>r;
    cout<<"input Y value:";
    for(int i=0;i<4;i++)
    {
        for(int j=0;j<4;j++)
        {
            cin>>Y[i][j];
        }
    }
```

Figure 1

```
for(int i=0;i<8;i++)
{
    for(int j=0;j<8;j++)
    {
        if(i%2==0 && j%2==0)
            A[i][j]=F(r+1);
        if(i%2!=0 && j%2!=0)
            A[i][j]=F(r-1);
        if(i%2==0 && j==i+1)
            A[i][j]=F(r);
        if(i%2!=0 && j==i-1)
            A[i][j]=F(r);
        if(i>=2 && i!=4 && i!=5 && j==i-2)
            A[i][j]=1;
        if(j>=2 && j!=4 && j!=5 && i==j-2)
            A[i][j]=1;
        if(i+j==3 || i+j==11)
            A[i][j]=0;
        if(i<=3 && j>=4)
            A[i][j]=Y[i][j-4];
        if (i>=4 && j<=3)
            A[i][j]=0;
    }
}
cout<<"\n Matrix A ";
for(int i=0;i<8;i++)
{
    cout<<"\n";
    for(int j=0;j<8;j++)
    {
        cout<<A[i][j]<<"\t";
    }
}
```

Figure 2

```
    for(int i=0;i<8;i++)
    {
        for(int j=0;j<2;j++)
        {
            if(i%2==0 && j==0)
                B[i][j]=F(r+1);
            if(i%2!=0 && j==1)
                B[i][j]=F(r-1);
            if(i%2==0 && j==1)
                B[i][j]=F(r);
            if(i%2!=0 && j==0)
                B[i][j]=F(r);

        }
    }
    cout<<"\n Matrix B";
    for(int i=0;i<8;i++)
    {
        cout<<"\n";
        for(int j=0;j<2;j++)
        {
            cout<<B[i][j]<<"\t";
        }
    }
}
```

Figure 3

Original message is encrypted byte by byte. Therefore, the plan text is converted to a block of 8 bits and then encrypted one by one. Suppose the original message is of length 'm'. If $m \equiv 0 (\mathrm{mod}\ 8)$ and $m \geq 8$, the plaintext is converted to cipher text byte by byte. Else the leftover bits in the plain text are filled with character space to complete a byte.

For a message of 8 bits we have,
C = Cipher text matrix of 8*2 order and
X = Plain text matrix of 8*2 order
where each row is a point equivalent to the assigned character on the Elliptic curve.

For a message of size greater than 8 bits, we divide the message into 'n' number of blocks each of length 8 bits. Then the plain text is written in the form of a matrix as $X = [X_1 X_2 \ \ldots \ X_n]$ of order 8*2n where X_i is a matrix of 8*2 order. The obtained Cipher text will be $C = [C_1 C_2 \ \ldots \ C_n]$ of order 8*2n, where C_i is a matrix of 8*2 order.

Encryption

The cipher text for the block of data can be obtained by computing

$$C_i = A * X_i + B \qquad [5]$$

where $[C_i]_{8*2}$, $[A]_{8*8}$, $[X_i]_{8*2}$ and $[B]_{8*2}$ are matrices for i = 1, 2,…, n. Then the final Cipher text is $C = [C_1 C_2 \ \ldots \ C_n]$

Decryption

The plain text is obtained by computing

$$X_i = A^{-1} * (C_i - B) \quad [6]$$

where $[C_i]_{8*2}$, $[A^{-1}]_{8*8}$and$[B]_{8*2}$ are matrices for i = 1, 2,…, n for each block of data. Then the final plain text is $X = [X_1 X_2 \ \ldots \ X_n]$.

Example

Let us consider the Elliptic curve $E_{29}(2,3)$.

Let G = (1,8) and $Y = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$ where G and Y are public key.

TABLE 1: A bijective map $E_p(q, r) \rightarrow$ Set of English alphabets A to Z (18)

Point on $E_{29}(2,3)$		Character
1P	(1,8)	A
2P	(22,9)	B
3P	(11,15)	C
4P	(23,23)	D
5P	(9,5)	E
6P	(6,12)	F
7P	(18,19)	G
8P	(5,15)	H
9P	(17,22)	I
10P	(24,19)	J
11P	(13,14)	K
12P	(8,3)	L
13P	(14,22)	M
14P	(27,22)	N
15P	(26,12)	O
16P	(3,23)	P
17P	(16,10)	Q
18P	(28,0)	R
19P	(16,19)	S
20P	(3,6)	T
21P	(26,17)	U
22P	(27,7)	V
23P	(14,7)	W
24P	(8,26)	X
25P	(13,15)	Y
26P	(24,10)	Z
27P	(17,7)	Space

The value of F is: $F = \begin{bmatrix} F_4 & F_3 \\ F_3 & F_2 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}$.

Then $F' = \begin{bmatrix} 3 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \\ 1 & 0 & 3 & 2 \\ 0 & 1 & 2 & 1 \end{bmatrix}$, $A = \begin{bmatrix} 3 & 2 & 1 & 0 & 2 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 3 & 2 & 0 & 0 & 2 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \end{bmatrix}$.

Suppose that the original message is: "DON IS IN LONDON." Then $m = 16$. Since $16 \equiv 0 (\mathrm{mod}\ 8)$ and $16 \geq 8$, therefore, the message can be split into two blocks of size 8 bits each for encryption and decryption as:

TABLE 2

Block 1	D	O	N	I	S		I
Block 2	N		L	O	N	D	O	N

For the 1st block of data, the value of X1 = $\begin{bmatrix} 23 & 23 \\ 26 & 12 \\ 27 & 22 \\ 17 & 7 \\ 17 & 22 \\ 16 & 19 \\ 17 & 7 \\ 17 & 22 \end{bmatrix}$

For the 2nd block of data, the value of X2 = $\begin{bmatrix} 27 & 22 \\ 17 & 7 \\ 8 & 3 \\ 26 & 12 \\ 27 & 22 \\ 23 & 23 \\ 26 & 12 \\ 27 & 22 \end{bmatrix}$

The plain text is $X = [X_1 X_2]$ = $\begin{bmatrix} 23 & 23 & 27 & 22 \\ 26 & 12 & 17 & 7 \\ 27 & 22 & 8 & 3 \\ 17 & 7 & 26 & 12 \\ 17 & 22 & 27 & 22 \\ 16 & 19 & 23 & 23 \\ 17 & 7 & 26 & 12 \\ 17 & 22 & 27 & 22 \end{bmatrix}$

Encryption (19)

$C_1 = A * X_1 + B$(Skewed Affine Cipher)

$$C_1 = \begin{bmatrix} 3 & 2 & 1 & 0 & 2 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 3 & 2 & 0 & 0 & 2 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \end{bmatrix} * \begin{bmatrix} 23 & 23 \\ 26 & 12 \\ 27 & 22 \\ 17 & 7 \\ 17 & 22 \\ 16 & 19 \\ 17 & 7 \\ 17 & 22 \end{bmatrix} + \begin{bmatrix} 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 182 & 159 \\ 121 & 103 \\ 172 & 117 \\ 131 & 107 \\ 100 & 111 \\ 67 & 85 \\ 102 & 87 \\ 67 & 55 \end{bmatrix} + \begin{bmatrix} 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 185 & 161 \\ 123 & 104 \\ 175 & 119 \\ 133 & 108 \\ 103 & 113 \\ 69 & 86 \\ 105 & 89 \\ 69 & 56 \end{bmatrix}$$

Similarly, $C_2 = A * X_2 + B$

$$C_2 = \begin{bmatrix} 3 & 2 & 1 & 0 & 2 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 3 & 2 & 0 & 0 & 2 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \end{bmatrix} * \begin{bmatrix} 27 & 22 \\ 17 & 7 \\ 8 & 3 \\ 26 & 12 \\ 27 & 22 \\ 23 & 23 \\ 26 & 12 \\ 27 & 22 \end{bmatrix} + \begin{bmatrix} 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 177 & 127 \\ 143 & 109 \\ 155 & 79 \\ 113 & 69 \\ 153 & 124 \\ 104 & 89 \\ 159 & 102 \\ 102 & 69 \end{bmatrix} + \begin{bmatrix} 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 180 & 129 \\ 145 & 110 \\ 158 & 81 \\ 115 & 70 \\ 156 & 126 \\ 106 & 90 \\ 162 & 104 \\ 104 & 70 \end{bmatrix}$$

$$C = [C_1 \quad C_2] = \begin{bmatrix} 185 & 161 & 180 & 129 \\ 123 & 104 & 145 & 110 \\ 175 & 119 & 158 & 81 \\ 133 & 108 & 115 & 70 \\ 103 & 113 & 156 & 126 \\ 69 & 86 & 106 & 90 \\ 105 & 89 & 162 & 104 \\ 69 & 56 & 104 & 70 \end{bmatrix}$$

Decryption (19)

$X_1 = A^{-1} * (C_1 - B)$

$$= \begin{bmatrix} 0.25 & 0 & 0.25 & -0.5 & -0.75 & 1 & -0.25 & 0.5 \\ 0 & 0.25 & -0.5 & 0.75 & 1 & -1.75 & 0.5 & -0.75 \\ 0.25 & -0.5 & 0.25 & 0 & -0.25 & 0.5 & -0.75 & 1 \\ -0.25 & 0.75 & 0 & 0.25 & 0.5 & -0.75 & 1 & -1.75 \\ 0 & 0 & 0 & 0 & 0.25 & 0 & 0.25 & -0.5 \\ 0 & 0 & 0 & 0 & 0 & 0.25 & -0.5 & 0.75 \\ 0 & 0 & 0 & 0 & 0.25 & -0.5 & 0.25 & 0 \\ 0 & 0 & 0 & 0 & -0.5 & 0.75 & 0 & 0.25 \end{bmatrix} * \left(\begin{bmatrix} 185 & 161 \\ 123 & 104 \\ 175 & 119 \\ 133 & 108 \\ 103 & 113 \\ 69 & 86 \\ 105 & 89 \\ 69 & 56 \end{bmatrix} - \begin{bmatrix} 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \end{bmatrix} \right)$$

$$= \begin{bmatrix} 23 & 23 \\ 26 & 12 \\ 27 & 22 \\ 17 & 7 \\ 17 & 22 \\ 16 & 19 \\ 17 & 7 \\ 17 & 22 \end{bmatrix}$$

Similarly, $X_2 = A^{-1} * (C_2 - B)$

$$= \begin{bmatrix} 0.25 & 0 & 0.25 & -0.5 & -0.75 & 1 & -0.25 & 0.5 \\ 0 & 0.25 & -0.5 & 0.75 & 1 & -1.75 & 0.5 & -0.75 \\ 0.25 & -0.5 & 0.25 & 0 & -0.25 & 0.5 & -0.75 & 1 \\ -0.25 & 0.75 & 0 & 0.25 & 0.5 & -0.75 & 1 & -1.75 \\ 0 & 0 & 0 & 0 & 0.25 & 0 & 0.25 & -0.5 \\ 0 & 0 & 0 & 0 & 0 & 0.25 & -0.5 & 0.75 \\ 0 & 0 & 0 & 0 & 0.25 & -0.5 & 0.25 & 0 \\ 0 & 0 & 0 & 0 & -0.5 & 0.75 & 0 & 0.25 \end{bmatrix} * \left(\begin{bmatrix} 180 & 129 \\ 145 & 110 \\ 158 & 81 \\ 115 & 70 \\ 156 & 126 \\ 106 & 90 \\ 162 & 104 \\ 104 & 70 \end{bmatrix} - \begin{bmatrix} 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \\ 3 & 2 \\ 2 & 1 \end{bmatrix} \right)$$

$$= \begin{bmatrix} 27 & 22 \\ 17 & 7 \\ 8 & 3 \\ 26 & 12 \\ 27 & 22 \\ 23 & 23 \\ 26 & 12 \\ 27 & 22 \end{bmatrix}$$

Therefore, $X = [X_1\ X_2] = \begin{bmatrix} 23 & 23 & 27 & 22 \\ 26 & 12 & 17 & 7 \\ 27 & 22 & 8 & 3 \\ 17 & 7 & 26 & 12 \\ 17 & 22 & 27 & 22 \\ 16 & 19 & 23 & 23 \\ 17 & 7 & 26 & 12 \\ 17 & 22 & 27 & 22 \end{bmatrix}$

TABLE 3: Original Message

Points on $E_{29}(2,3)$	Plain text character
(23,23)	D
(26,12)	O
(27,22)	N
(17,7)	Space
(17,22)	I
(16,19)	S
(17,7)	Space
(17,22)	I
(27,22)	N
(17,7)	Space
(8,3)	L
(26,12)	O
(27,22)	N
(23,23)	D
(23,12)	O
(27,22)	N

Cryptanalysis

The Elliptic curve used in the process remains confidential, increasing the difficulty level for cryptanalysis. The non-singular block matrix generated with the sub-matrix formed using the compatible Fibonacci and identity matrices can also be attacked only when the private key is disclosed. Thus carrying a brute force attack is impossible.

As the data is encrypted in the form of matrices, therefore the algorithm retains the Avalanche effect. Also, the same plain text characters at different indices would produce various cipher texts. Thus the algorithm is resistant to attacks by frequency analysis.

Conclusions

The mathematical concept of the existence of inverses in specific matrices such as the Fibonacci and particular case of Block matrix has served as the base for developing the above method with an addition to the skewed Affine Cipher. The memory management is also focused in the paper as the data is encrypted by communicating 8 characters in a single stretch. Thus two-level security is provided. A robust key exchange protocol is required to exchange the secret key on which the entire security of the cryptosystem relies.

Acknowledgments

We extend our sincere thanks to GITAM for supporting our research work by providing Dr. M.V.V.S. Murthi research fellowship.

References

1. AbdAllah A. ElHabshy, *IJNS*, **21**(5), p.812-818 (2019).
2. Behrouz A Forouzan and Debdeep Mukhopadhyay ,*Cryptography and network security*, Third Edition, p.283-290, McGraw Hill Education.
3. Dawahdeh Z. E, Yaakob S. N, and Bin Othman R. R, *Journal of King Saud University , Computer and Information Sciences*, **30**(3) (2017).
4. Douglas R. Stinson and Maura B. Paterson, *Cryptography Theory and Practice*, Fourth Edition, p.278-286, CRC Press, Taylor & Francis Group.
5. D. Sravana Kumar, Ch. Suneetha, and A. Chandrasekhar, *IJDPS*, **3**(1) (2012).
6. Hassan Naraghi and Mozhgan Mohtari, *JMR,* **4**(1), p.67-77 (2012).
7. Inam, S and Ali R, *Neural Comput & Applic*, **29**, p.1279–1283 (2018). https://doi.org/10.1007/s00521-016-2745-2
8. John Silvester, *The Mathematical Gazette,* **84**(501), p.460-467 (2000).
9. Kalika Prasad and Hrishikesh Mahato ,Cryptography using generalized Fibonacci matrices with Affine-Hill cipher, Available online at arXiv:2003.11936v1 [cs.CR] 25 Mar 2020
10. Komal Agrawal and Anuj Gera, *IJCA*, **106**(1), p.18-24 (2014).
11. Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, *Eleventh IMCIP-2015, Procedia Computer Science*, **54**, p.472 – 481(2015).
12. Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, *Eleventh IMCIP-2015*, Procedia Computer Science, **54**, p.73 – 82(2015).
13. Mohamed Abdel Hafez Bakr, Amr Mokhtar, and Ali Takieldeen, *IJIEEE*, **6**(7) (2018).
14. Mohammed Amin Almaiah, Ziad Dawahdeh, Omar Almomani, Adeeb Saaidah, Ahmad Al-khasawneh, and Saleh Khawatreh, *IJECE*, **10**(6), p.6461-6471(2020).
15. Neha Sharma and Sachin Chrgaiya, *IJCA*, **108**(11), p.34-37 (2014).
16. Wade Trappe and Lawrence C. Washington, *Introduction to Cryptography with Coding Theory*, Second Edition, p.347-363, Pearson Education International.
17. https://www.statlect.com/matrix-algebra/determinant-of-block-matrix
18. http://www.christelbach.com/ECCalculator.aspx

19. https://www.calculator.net/matrix-calculator.html