Commun. Combin., Cryptogr. & Computer Sci., 2 (2022), 94–104

ISSN:2783-5456

Communications in Combinatorics, Cryptography & Computer Science

Journal Homepage: http://cccs.sgh.ac.ir

A Public-Key Cryptographic Model Based on Hybrid Key Exchange Technique using Affine-Hill Cipher

Kshitish Kumar Mohanta[a,*], Deena Sunil Sharanappa[a]

[a]Department of Mathematics, Indira Gandhi National Tribal University, Amarkantak, 484887, Anuppur, Madhya Pradesh, India

Abstract

In this paper, a hybrid method for creating key matrices using the multi-key exchange algorithm was suggested. It combines the ElGamal and Elliptic Curve Diffe Hellman (ECDH) algorithms. The key matrix for encryption and decryption uses the generalized Fibonacci matrix modulo $\mathfrak{p}$ and the inverse of the generalized Fibonacci matrix modulo $\mathfrak{p}$. Generalized Fibonacci sequences are used to construct these matrices. With the help of the proposed combined algorithm, we only need to sent the order and power of the generalized Fibonacci matrix and the seeds of the generalized Fibonacci sequence, rather than the entire key matrix. The Affine Hill Cipher technique is used in this public key cryptography model to encrypt plain text and decrypt cipher text. The proposed method increases security strength of the model due to use of four secrete integers $\mathfrak{a}, \mathfrak{b}, (\mathfrak{n}, \mathfrak{m})$.

Keywords: Public key cryptography, Elliptic Curve Diffie-Hellman(ECDH) Algorithm, ElGamal Algorithm, Generalized Fibonacci matrix, Affine-Hill Cipher.

2020 MSC: 11B39, 11T71, 94A60.

1. Introduction

The urge to communicate secretly is at least as old as writing and may be traced back to the start of civilization. Many ancient societies created secret communication systems, including Egypt, India, China, and Japan, but the origins of cryptology, i.e "the science and art of secure communication", remain unknown. Cryptography is the study of methods for sending messages or information in secret so that only the intended/authorized recipient can remove the disguise and read the message. The method to obtain the ciphertext from plaintext is called encryption and the reverse method is called decryption. There are several techniques for encryption scheme. ElGamal [15] and Elliptic Curve Cryptography (ECC) [2, 3] are the newest member in the family of public key cryptosystem. The principal cause for this system is its higher security level and has fewer computations as compared to existing public-key cryptosystem. For those reasons it has attracted the attention of the mathematicians, cryptographers, and computers makers around the world.

In 1929, mathematician Lester Hill has developed the polygraphic substitution ciphers which is known as Hill cipher [3, 16]. The concept of public key cryptography using Hill's Cipher was proposed by Viswanath

*Corresponding author
Email addresses: kshitishkumar.math@gmail.com (Kshitish Kumar Mohanta), deena.sunil@igntu.ac.in (Deena Sunil Sharanappa)

Received: November 3, 2022 Revised: November 10, 2022 Accepted: November 21, 2022

& Kumar [9]. They have used a system of rectangular matrix in which they have developed a public key cryptography with Hill cipher and the inverse key matrix is obtained by using MoorePenrose Inverse (Pseudo Inverse) method. Sundarayya & Prasad [12] have extended the same research [9] to develop a public key cryptosystem using Affine-Hill Cipher. They have used two or more digital signatures to increased security of the system. Recently, Fibonacci matrix [5, 8, 1], Lucas matrix [6] and Lucas-Balancing number [13, 14] have been used as a key matrix for encryption and decryption process in public key cryptography and briefly describe their security strength.

In this parer, the generalized Fibonacci matrix is taken as encryption matrix whereas the It's inverse is taken as decryption matrix. These matrices are created based on the secrete key share using hybrid public key exchange technique. We used a hybrid key exchange algorithm based on ElGamal and Elliptic curve Diffie-Hellman key exchange techniques. The system uses 67 alphabets, characters & numbers as shown in Table (1).

Table 1: Digital equivalent of Character & number

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
R	S	T	U	V	W	X	Y	Z	a	b	c	d	e	f	g	h
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
z	0	1	2	3	4	5	6	7	8	9	"space"		,	.	!	?
51	52	53	54	55	56	57	58	59	60	61	62		63	64	65	66

This paper is contained the following section. Section (2) discuss about Generalized Fibonacci matrices and its inverse. Section (3) discus ElGamal technique, elliptic curve Diffie-Hellman key exchange technique and proposed combined technique for key generation. Section (4) discuss about the encryption and decryption technique and block creation technique. The algorithm for the proposed technique discussed in Section (5). Section (6) provides an example to show its validity and applicability of the proposed model. Section (7) discuss about the strength of the proposed cryptosystem. Finlay, the conclusion of this paper discuss in section (8).

2. Generalized Fibonacci matrix and it's Inverse

Generalized Fibonacci number is defined by $f_{n+1}=f_n+f_{n-1};\ n\geqslant 1$ with seeds $f_0=a$ and $f_1=b$. The n^{th} generalized Fibonacci number f_n can be calculated as

$$f_n = \mu_1\alpha^n + \mu_2\beta^n \tag{2.1}$$

where $\alpha = \dfrac{1+\sqrt{5}}{2}, \beta = \dfrac{1-\sqrt{5}}{2}$ and $\mu_1 = \dfrac{\sqrt{5}a+(2b-a)}{2\sqrt{5}}, \mu_2 = \dfrac{\sqrt{5}a-(2b-a)}{2\sqrt{5}}$. For different choice of a and b gives different number sequences. Taking $a=1$ and $b=1$ in equation (2.1) gives famous Fibonacci number sequence [16]. The first few terms of the sequence are 0, 1, 1, 2, 3, 5, 8, 13,$\cdots$. Similarly, The first few terms of the Lucas Number sequences[16] are 2, 1, 3, 4, 7, 11, 18, 29, $\cdots$, by choice of $a=2$ and $b=1$ in equation (2.1).

Definition 2.1. The Generalized Fibonacci matrix [11] is defined as

$$\mathfrak{F}_n = \begin{cases} f_{i-j+1}, & i-j\geqslant 0 \\ 0, & i-j<0 \end{cases} = \begin{bmatrix} f_1 & 0 & 0 & \cdots & 0 \\ f_2 & f_1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ f_n & f_{n-1} & f_{n-2} & \cdots & f_1 \end{bmatrix}, \tag{2.2}$$

where $f_0 = a$ and $f_1 = b$.

Example 2.1. The 5×5 generalized Fibonacci matrix is equal to

$$\mathfrak{F}_5 = \begin{bmatrix} b & 0 & 0 & 0 & 0 \\ a+b & b & 0 & 0 & 0 \\ a+2b & a+b & b & 0 & 0 \\ 2a+3b & a+2b & a+b & b & 0 \\ 3a+5b & 2a+3b & a+2b & a+b & b \end{bmatrix}.$$

For $a = 0$ and $b = 1$ in equation (2.2), which gives Fibonacci matrix [11]. For $a = 2$ and $b = 1$ in equation (2.2), which gives Lucas matrix [18].

Definition 2.2. For $b \neq 0$, The inverse of $n \times n$ generalized Fibonacci matrix [11] is defined as

$$\mathfrak{F}_n^{-1} = \begin{cases} (-1)^{i-j} \dfrac{a^2+ab-b^2}{b^{i-j+1}} a^{i-j-2}, & \text{if } i \geqslant j+2 \\ -\dfrac{a+b}{b^2}, & \text{if } i = j+1 \\ \dfrac{1}{b}, & i = j \\ 0, & \text{otherwise} \end{cases}. \tag{2.3}$$

Example 2.2. For $b \neq 0$, The inverse of 5×5 generalized Fibonacci matrix is equal to

$$\mathfrak{F}_5^{-1} = \begin{bmatrix} \dfrac{1}{b} & 0 & 0 & 0 & 0 \\ -\dfrac{a+b}{b^2} & \dfrac{1}{b} & 0 & 0 & 0 \\ \dfrac{a^2+ab-b^2}{b^3} & -\dfrac{a+b}{b^2} & \dfrac{1}{b} & 0 & 0 \\ \dfrac{-a(a^2+ab-b^2)}{b^4} & \dfrac{a^2+ab-b^2}{b^3} & -\dfrac{a+b}{b^2} & \dfrac{1}{b} & 0 \\ \dfrac{a^2(a^2+ab-b^2)}{b^5} & \dfrac{-a(a^2+ab-b^2)}{b^4} & \dfrac{a^2+ab-b^2}{b^3} & -\dfrac{a+b}{b^2} & \dfrac{1}{b} \end{bmatrix}.$$

For $a = 0$ and $b = 1$ in equation (2.3), which gives the inverse of Fibonacci matrix, introduced by G. Y. Lee et al. [4] and defined as

$$\mathfrak{F}_n^{-1} = \begin{cases} 1, & \text{if } i = j \\ -1, & \text{if } i = j+1 \\ -1, & \text{if } i = j+2 \\ 0, & \text{otherwise} \end{cases} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ -1 & 1 & 0 & 0 & \cdots & 0 \\ -1 & -1 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & & \cdots & 1 \end{bmatrix}.$$

Similarly, For $a = 2$ and $b = 1$ in equation (2.3), which gives the inverse of $n \times n$ Lucas matrix introduced by Z. Zhang and Y. Zahang [18] and is defined as

$$\mathcal{L}_n^{-1} = \begin{cases} 5(-1)^{i-j} 2^{i-j-2}, & \text{if } i \geqslant j+2 \\ -3, & \text{if } i = j+1 \\ 1, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}.$$

Theorem 2.3. Let p be a prime, $A = (a_{ij})_{n\times n}$ and $B = (b_{ij})_{n\times m}$ be the matrices, then

(a) $A \pmod p = (a_{ij} \pmod p)_{n\times n}$.
(b) $AB \pmod p = [A \pmod p][B \pmod p] \pmod p$.
(c) $A^k \pmod p) = [A \pmod p]^k \pmod p$.
(d) The inverse of $A \pmod p$ exist iff $\det(A) \not\equiv 0 \pmod p$.

3. Generation of Key Matrix

This section contains three subsection to describe briefly the ElGamal key exchange technique, Elliptic curve Diffie-Hellman (ECDH) key exchange technique, and the proposed hybrid key exchange technique.

3.1. ElGamal Technique

ElGamal key exchange technique is a public key exchanged technique based on Deffie-Hellman technique [17] which was proposed by T. Elgamal [15] in 1984. Here we choose an arbitrary prime p and select a primitive root (α) of $\mathbb{Z}_p$. The domain parameter is (p, α), where α is the primitive root of $\mathbb{Z}_p$. Now Alice and bob create public key and private key using this technique given in Table (2).

Table 2: ElGamal algorithm

Select the domain parameter (p, α)	
Alice	Bob
Choose the private key $K_{pr,A} = d \in \{2, 3, \cdots, p-2\}$ and calculate the public key $K_{pub,A}=\beta$ where $\beta=\alpha^d (\mathrm{mod}\ p)$.	Choose the private key $K_{pr,B} = e \in \{2, 3, \cdots, p-2\}$ and calculate the public key $K_{pub,B} = \gamma = \alpha^e (\mathrm{mod}\ p)$.
Share each other their public key $K_{pub,B} \longleftarrow \longrightarrow K_{pub,A}$	
Calculate together	
$a = \gamma^d \pmod p$.	$a = \beta^e \pmod p$.

3.2. ECDH Technique

Elliptic curve Diffie-Hellman [10, 2] key exchange technique is a public key exchange process based on Elliptic Curve. Here we choose an Elliptic curve modulo p and select a primitive element in the elliptic curve. Suppose Alice and Bob want to exchange key. Let p be a prime and $E: y^2 \equiv x^3 + ux + v \pmod p$ be an elliptic curve. Let $Q = (x_Q, y_Q)$ be a primitive element of E and $X = \{2, 3, \cdots, \#E - 1\}$ where $\#E$ is the order of elliptic curve. The domain parameter are $(p, a, b, Q = (x_Q, y_Q))$. Now Alice and bob create private key and public key using this technique given in Table (3).

Table 3: ECDH algorithm

Select the domain parameter (p, u, v, Q).	
Alice	Bob
Choose private key $K_{pr,A} = \beta \in X$ and calculate public key $K_{pub,A} = A = \beta Q$.	Choose private key $K_{pr,B} = \alpha \in X$ and calculate the public key $K_{pub,B}=B=\alpha Q$.
Share each other their public key $K_{pub,B} = B \longleftarrow \longrightarrow K_{pub,A} = A$	
Calculate together	
$\beta B = (n, m)$	$\alpha A = (n, m)$

3.3. Technique for this Model

This technique defined in Table (4), is a combination of ElGamal Algorithm and ECDH Algorithm. Let p be a prime and $E: y^2 \equiv x^3 + ux + v \pmod p$ be an elliptic curve. and $X = \{2, 3, \cdots, \#E - 1\}$ where $\#E$

Table 4: Combined algorithm

Select the domain parameter (p, α, u, v, Q)	
Alice	Bob
Choose the Private key $K_{pr,A} = (d_1, d_2, \beta)$, where $d_1, d_2 \in \{2, 3, \cdots, p-2\}$ and $\beta \in X$. and calculate the Public key $K_{pub,A} = (\delta_1, \delta_2, A)$, where $\delta_1 = \alpha^{d_1} \pmod p, \delta_2 = \alpha^{d_2} \pmod p$ and $A = \beta Q$.	Choose the private key $K_{pr,B} = (e, c)$ where $e \in \{2, 3, \cdots, p-2\}$ and $c \in X$. and calculate the public key $K_{pub,B} = (\gamma, B)$ where $\gamma = \alpha^e \pmod p$ and $B = cQ$
Share each other their public key $K_{pub,B} \longleftarrow \longrightarrow K_{pub,A}$	
Calculate together secretly	
$a = \gamma^{d_1} \pmod p$, $b = \gamma^{d_2} \pmod p$, $(n, m) = \beta B$	$a = \delta_1^e \pmod p$, $b = \delta_2^e \pmod p$, $(n, m) = cA$.

is the order of elliptic curve. Let $\alpha \in \{2, 3, \cdots, p-2\}$ be a primitive element of $\mathbb{Z}_p$ and $Q = (x_Q, y_Q)$ be the primitive element of E. The domain parameter is (p, α, u, v, Q).

Now using $a, b, (n, m)$ they create their secrete encryption and decryption key matrix. The Encryption key $K = \mathfrak{F}_n^m \pmod{67}$ and Decryption key $K^{-1} = (\mathfrak{F}_n^{-1})^m \pmod{67}$.

4. Technique for Encryption and Decryption

Affine-Hill cipher is a polygraphic substitution block cipher, which is the extension of the concept of the Hill Cipher [7, 2]. The encryption and decryption technique for this cipher is given below:

$$E_K(P_i): \ C_i \equiv P_i K + B_i \pmod{67} \tag{4.1}$$

$$D_K(C_i): \ P_i \equiv (C_i - B_i)K^{-1} \pmod{67} \tag{4.2}$$

Where P_i, C_i and $B_i = [f^i_{m+1} \ f^i_{m+2} \ \cdots \ f^i_{m+n}]$ are $1 \times n$ matrices, K be the key matrix of order n and $E_K(P)$ and $D_K(C)$ represents encryption function and decryption function respectively. The Secret number n represent the order of the matrix and length of each block. Let l be the length of the plain text string. Then number of block are $\lceil \frac{l}{n} \rceil$, where $\lceil \cdot \rceil$ is the ceiling function. In the last block, to complete its length we use dummy text i.e "space".

Remark 4.1. It is important to choose b in such a way that $b \not\equiv 0 \pmod{67}$ so that the inverse of the generalized Fibonacci matrix exist.

5. Algorithm for proposed model

The algorithm for generating encryption key in algorithm 1 for encryption in algorithm 2 of plain text into cipher text and the algorithm for decryption key in algorithm 3 for decryption in algorithm 4 of cipher text into plain text are given below. The flow chart for the proposed model is presented in Figure 1.

Algorithm 1 Encryption Key K

Require: Domain parameter (p, α, u, v, Q)
Ensure: K

Choose $d_1, d_2 \in \{2, 3, \cdots, p-2\}$, $\beta \in X$.
$K_{pr,A} \Leftarrow (d_1, d_2, \beta)$.
$\delta_1 \Leftarrow \alpha^{d_1} (\mathrm{mod}\ p), \delta_2 \Leftarrow \alpha^{d_2} (\mathrm{mod}\ p)$, $A \Leftarrow \beta Q$.
$K_{pub,A} \Leftarrow (\delta_1, \delta_2, A)$.
Send $\rightarrow K_{pub,A}$.
Received $\leftarrow K_{pub,B}$.
$a \Leftarrow \gamma^{d_1} \bmod(p), b \Leftarrow \gamma^{d_2} \bmod(p), (n, m) \Leftarrow \beta B$.
for $i \leftarrow 1$ to n do
    for $j \leftarrow 1$ to n do
        if $i - j > 0$ then
            $a_{ij} \Leftarrow (\frac{1+\sqrt{5}}{2})^{i-j+1}(\frac{\sqrt{5}a+2b-a}{2\sqrt{5}}) + (\frac{1-\sqrt{5}}{2})^{i-j+1}(\frac{\sqrt{5}a-2b+a}{2\sqrt{5}})$
        else
            $a_{ij} \Leftarrow 0$
        end if
    end for
end for
$\mathfrak{F}_n \Leftarrow (a_{ij})$
return $K \Leftarrow \mathfrak{F}_n^m \ (\mathrm{mod}\ 67)$.

Algorithm 2 Encryption

Require: Plain text P, and K.
Ensure: Cipher text C.

$l \Leftarrow \mathrm{length}(P)$.
$k \Leftarrow \lceil \frac{l}{n} \rceil$.
$P \Leftarrow (P_1 P_2 \cdots P_k)$.
for $i \leftarrow 1$ to k do
    for $j \leftarrow 1$ to n do
        $B_{ij} \Leftarrow f^i_{m+j}$
    end for
    $B_i \Leftarrow (B_{ij})$
    $C_i \Leftarrow P_i K + B_i \ (\mathrm{mod}\ 67)$.
end for
return $C = (C_1 C_2 \cdots C_k)$.

Algorithm 3 Decryption Key K^{-1}

Require: Domain parameter (p, α, u, v, Q)
Ensure: K^{-1}

Choose $e \in \{2, 3, \cdots, p-2\}$, $c \in X$.
$K_{pr,B} \Leftarrow (e, c)$.
$\gamma \Leftarrow \alpha^e (\mathrm{mod}\ p)$, $B \Leftarrow cQ$.
$K_{pub,B} \Leftarrow (\gamma, B)$.
Send $\rightarrow K_{pub,B}$.
Received $\leftarrow K_{pub,A}$.
$a \Leftarrow \delta_1^e \bmod(p), b \Leftarrow \delta_2^e \bmod(p), (n, m) \Leftarrow cA$.
for $i \leftarrow 1$ to n do
    for $j \leftarrow 1$ to n do
        if $i \geqslant j-2$ then
            $a_{ij} \Leftarrow (-1)^{i-j} \frac{a^2+ab-b^2}{b^{i-j+1}} a^{i-j-2}$
        else if $i = j+1$ then
            $a_{ij} \Leftarrow -\frac{a+b}{b^2}$
        else if $i = j$ then
            $a_{ij} \Leftarrow \frac{1}{b}$
        else
            $a_{ij} \Leftarrow 0$
        end if
    end for
end for
$\mathfrak{F}_n^{-1} \Leftarrow (a_{ij})$
return $K^{-1} \Leftarrow \mathfrak{F}_n^{-m} \pmod{67}$.

Algorithm 4 Decryption

Require: Cipher text C, and K^{-1}
Ensure: Plain text P

$l \Leftarrow \mathrm{length}(C)$.
$k \Leftarrow \lceil \frac{l}{n} \rceil$.
$C \Leftarrow (C_1 C_2 \cdots C_k)$.
for $i \leftarrow 1$ to k do
    for $j \leftarrow 1$ to n do
        $B_{ij} \Leftarrow f_{m+j}^i$
    end for
    $B_i \Leftarrow (B_{ij})$
    $P_i \Leftarrow (C_i - B_i) K^{-1} \pmod{67}$.
end for
return $P = (P_1 P_2 \cdots P_k)$.

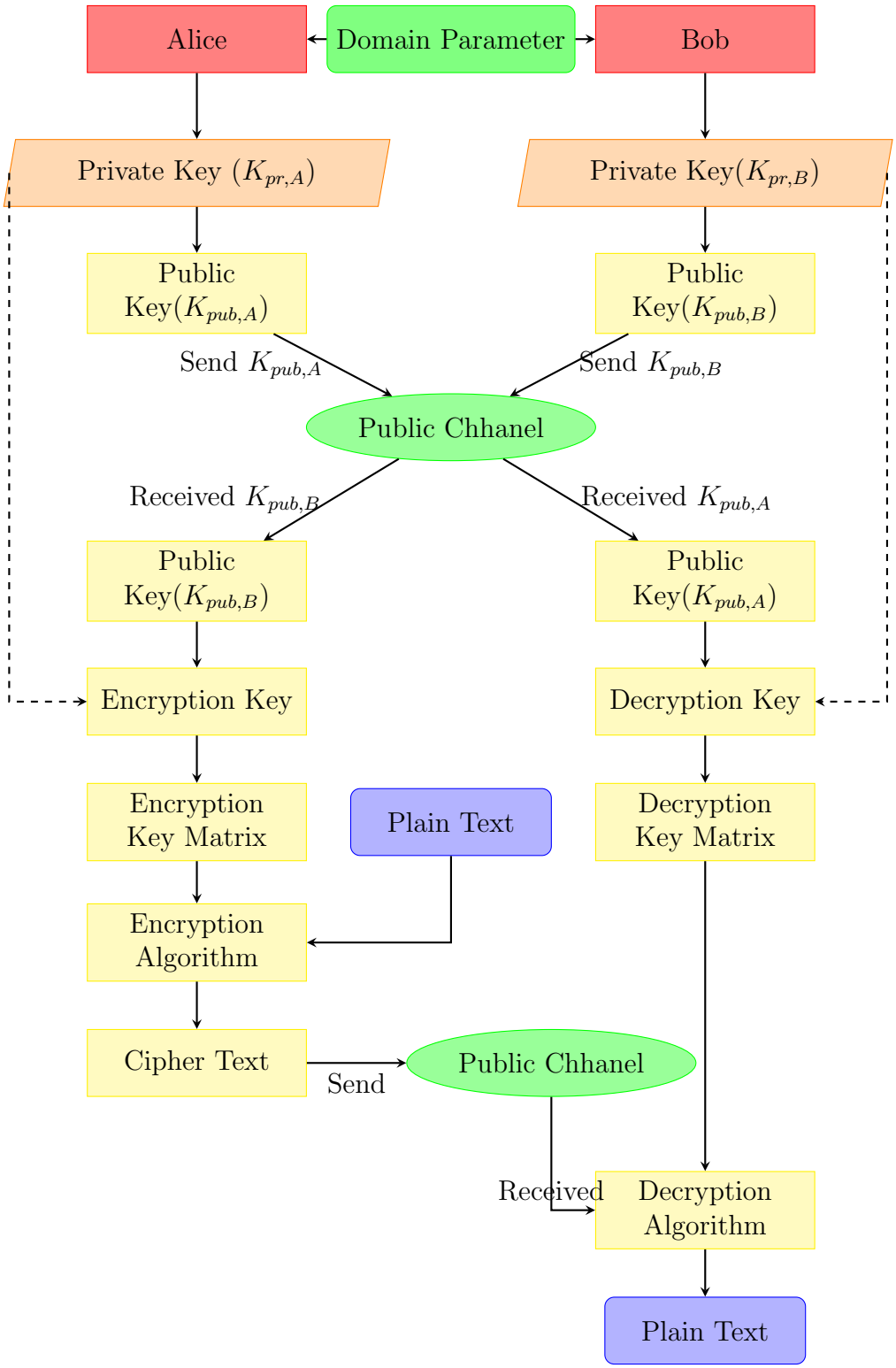

Figure 1: Encryption and decryption technique

6. Numerical Example

Suppose Alice want to communicate with Bob secretly in insecure channel. So first Alice calculate the encryption key matrix K using equation (2.2) and hybrid algorithm given in Table (4). Then encrypt the message (or "plaintext") P with the help of key matrix K. Similarly Bob calculate the decryption key matrix K^{-1}using equation (2.3) and hybrid algorithm given in Table (4) and decrypt the ciphertext which was encrypted by Alice.

Suppose Alice want to send the plain text is $\mathsf{P} = \mathsf{COVID19}$ to Bob secretly in an unsecured channel.

For Secret Key Exchange

Let the Domain Parameter is $(17, 5, 2, 2, (5, 1))$.

Alice and Bob choose their public key $\mathsf{K}_{\mathtt{pr},\mathtt{A}} = (\mathsf{d}_1, \mathsf{d}_2, \beta) = (10, 13, 6)$ and $\mathsf{K}_{\mathtt{pr},\mathtt{B}} = (\mathsf{e}, \mathsf{c}) = (14, 3)$. Calculate the private key for Alice and Bob $\mathsf{K}_{\mathtt{pub},\mathtt{A}} = (\delta_1, \delta_2, \mathsf{B}) = (9, 3, (16, 13))$ and $\mathsf{K}_{\mathtt{pub},\mathtt{B}} = (\gamma, \mathsf{A}) = (15, (10, 6))$. Now using the technique given in the Table (4), together calculate secret key $\mathfrak{a} = 4, \mathfrak{b} = 2, (\mathfrak{n}, \mathfrak{m}) = (5, 16)$.

For Encryption key matrix:

Now, Alice choose the secrete key and construct the key matrix K using algorithm 1.

$$\mathsf{K} = \mathfrak{F}_5^{16}(\mathtt{mod}\ 67) = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 6 & 2 & 0 & 0 & 0 \\ 8 & 6 & 2 & 0 & 0 \\ 14 & 8 & 6 & 2 & 0 \\ 22 & 14 & 8 & 6 & 2 \end{bmatrix}^{16} (\mathtt{mod}\ 67) \equiv \begin{bmatrix} 10 & 0 & 0 & 0 & 0 \\ 11 & 10 & 0 & 0 & 0 \\ 50 & 11 & 10 & 0 & 0 \\ 19 & 50 & 11 & 10 & 0 \\ 62 & 19 & 50 & 11 & 10 \end{bmatrix}.$$

For Decryption key matrix:

Bob choose the secrete key and construct the key matrix K^{-1} using algorithm 3.

$$\begin{aligned} \mathsf{K}^{-1} &= (\mathfrak{F}_5^{-1})^{16}(\mathtt{mod}\ 67) \\ &= \begin{bmatrix} 2^{-1} & 0 & 0 & 0 & 0 \\ -3\times 2^{-1} & 2^{-1} & 0 & 0 & 0 \\ 5\times 2^{-1} & -3\times 2^{-1} & 2^{-1} & 0 & 0 \\ -5 & 5\times 2^{-1} & -3\times 2^{-1} & 2^{-1} & 0 \\ 10 & -5 & 5\times 2^{-1} & -3\times 2^{-1} & 2^{-1} \end{bmatrix}^{16} (\mathtt{mod}\ 67) \\ &\equiv \begin{bmatrix} 47 & 0 & 0 & 0 & 0 \\ 22 & 47 & 0 & 0 & 0 \\ 49 & 22 & 47 & 0 & 0 \\ 55 & 49 & 22 & 47 & 0 \\ 38 & 55 & 49 & 22 & 47 \end{bmatrix} \end{aligned}$$

For Encryption:

Consider the plain text $\mathsf{P} = \mathsf{COVID19}$. The plain text is divided into blocks of length $\mathfrak{n} = 5$ as follows: $\mathsf{P}_1 = [\mathsf{C}, \mathsf{O}, \mathsf{V}, \mathsf{I}, \mathsf{D}] = [2\ 14\ 21\ 8\ 3], \mathsf{P}_2 = [1, 9, \ , \ , \ ] = [53\ 61\ 62\ 62\ 62]$ and $\mathsf{B}_1 = [40\ 32\ 5\ 37\ 42], \mathsf{B}_2 = [59\ 19\ 25\ 29\ 22]$. Alice encrypt the plain text by using encryption algorithm 2 that is $\mathsf{C}_\mathsf{i} \leftarrow \mathsf{P}_\mathsf{i}\mathsf{K} + \mathsf{B}_\mathsf{i}(\mathtt{mod}\ 67)$

$$\begin{aligned} \mathsf{C}_1 &= \mathsf{P}_1\mathsf{K} + \mathsf{B}_1(\mathtt{mod}\ 67) \equiv [61\ 56\ 51\ 16\ 5] \sim (94\mathsf{zQF}), \\ \mathsf{C}_2 &= \mathsf{P}_2\mathsf{K} + \mathsf{B}_2(\mathtt{mod}\ 67) \equiv [2\ 28\ 5\ 58\ 39] \sim (\mathsf{CcF6}\mathfrak{n}), \end{aligned}$$

which gives cipher-text $\mathsf{C} = (\mathsf{C}_1\mathsf{C}_2) = (94\mathsf{zQFCcF6}\mathfrak{n})$. Now, Alice send this cipher text C to Bob.

For Decryption:

After receiving cipher text $\mathsf{C} = 94\mathsf{zQFCcF6}\mathfrak{n}$ from Alice, Bob decrpty the Cipher text by using decryption algorithm 4 that is $\mathsf{P}_\mathsf{i} \leftarrow (\mathsf{C}_\mathsf{i} - \mathsf{B}_\mathsf{i})\mathsf{K}^{-1}(\mathtt{mod}\ 67)$.

$$\mathsf{P}_1 = (\mathsf{C}_1 - \mathsf{B}_1)\mathsf{K}^{-1}(\mathtt{mod}\ 67) \equiv [2\ 14\ 21\ 8\ 3] \sim (\mathsf{COVID}),$$

$$P_2 = (C_2 - B_2)K^{-1} (\mathrm{mod}\ 67) \equiv [53\ 61\ 62\ 62\ 62] \sim (19 \qquad),$$

.

Thus, Bob recovered the plain text $P = (P_1P_2) = \mathrm{COVID19}$ sent by Alice successfully.

7. Complexity of this model

In cryptography, It is important to protect the original information from intruder about the key, plain text and cipher text. The types of main attacks are Brute force attack, Known Plain text attack, Cipher text only attack, etc. In Brute force attack, the intruder tries all possible integer combination to find the key matrix and checks which one of them returns the plain text. So it will be difficult to guess the key matrix K or K^{-1} exactly. The attacker try to guess the private key or to develop an algorithm so that they can decrypt any further message is called Known Plain text attack. Similarly, The attacker try to deduce the private key or plain text is called Cipher text only attack.

An opponent (say, Oscar) might use brute force to break our suggested approach by generating all feasible matrices. Oscar must verify $(67)^{mn}$ matrices because we are working on $\mathbb{F}_{67}$.

Example 7.1. Let $p = 67$, $m = 5$, and $n = 17$, Oscar must verify $67^{5\times17} = 67^{85} = 1.64572864947679 \times 10^{15}$ matrices, which is comparable too huge.

Similarly, the possible inverse matrix computation is too complicated. In our proposed methods secure against various known attacks. This method is not so complicated and it can be easily implemented in system. There does not exist any strong attack against ElGamal and elliptic cryptosystem if we choose carefully the prime and the elliptic curve. It gives high security as compared to other public key cryptosystem like RSA and DL schemes. In ECC, $160-256$ bit length can provide equivalent security to $1024-3072$ bit in RSA and DL. It required shortest time due to shortest bit length of ECC. We can add some Digital signatures to increase the security of the given model with the help of elliptic curve digital signature algorithm(ECDSA). It is obvious that by making prime p and (m, n) excessively big, it becomes nearly unbreakable. As a result, if the key space is wide, attacking the system using a Brute-force approach is problematic. In that instance, the attacker may attempt to analyses the ciphertext using various statistical tests.

8. Conclusion

In order to secure information transformation and to authenticate persons, devices, and systems to other systems, cryptography plays an essential role in our day-to-day activities. In the IOT world, it is utilized for everything, including online shopping, banking, and email client pings. Without cryptographic tools, our modern society would come to a standstill and all of our essential information would be available for subsequent exploitation. In this key exchange technique, we share four integer secretly, these are $a, b, (n, m)$, to create the encryption and decryption key matrix. Out of these two key a, b jointly share using ElGamal technique and to recover these two integer by intruder using Discrete logarithm problem (DLP), which is computationally infeasible. Other two integers (n, m) are shared together using ECDH technique. For suitable choice of p and elliptic curve it is not possible to break the system. The proposed method have large key space, computationally and mathematically easy and provide high level security due to use of multi-key exchange technique. Since it is a polygraphic cryptosystem and length of plain text and cipher text are different, hence it is secure against all known attack. The affine vector B_i different for each encryption so increase the security level. Here we need to send only the seeds of generalized Fibonacci sequence and order and power of the key matrix instead of sending the whole key matrix, so this method is simple and easily implemented as compared to other existing cryptosystem.

Declarations

The authors have no conflicts of interest.

References

[1] B. Prasad, FIBONACCI MATRICES AND HYBRID MATRIX CRYPTOGRAPHY, Discrete Mathematics, Algorithms and Applications, 6(1) (2014), 1450009. 1

[2] C. Paar, J. Pelzl, Understanding cryptography: a textbook for students and practitioners, Springer Science & Business Media, 2009. 1, 3.2, 4

[3] D.R. Stinson, Cryptography: theory and practice, Chapman and Hall/CRC, 2005. 1

[4] G.Y. Lee, J.S. Kim, S.G. Lee, Factorizations and eigenvalues of fibonacci and symmetric fibonacci matrices, Fibonacci Quarterly, 40 (2002), pp. 203–211. 2

[5] K. Prasad, H. Mahato, Cryptography using generalized fibonacci matrices with affine hill cipher, Journal of Discrete Mathematical Sciences and Cryptography, (2021), pp. 1–12. 1

[6] K. Prasad, H. Mahato, M. Kumari, A novel public key cryptography based on generalized Lucas matrices, arXiv preprint arXiv:2202.08156, (2022). 1

[7] L.S. Hill, Cryptography in an algebraic alphabet, The American Mathematical Monthly, 36 (1929), pp. 306–312. 4

[8] M. Kumari, J. Tanti, On the role of the Fibonacci matrix as key in modified ECC, arXiv preprint arXiv:2112.11013, (2021). 1

[9] M. Viswanath, M.R. Kumar, A public key cryptosystem using hiil's cipher, Journal of Discrete Mathematical Sciences and Cryptography, 18 (2015), pp. 129–138. 1

[10] N. Mehibel, M. Hamadouche, A new approach of elliptic curve Diffie-Hellman key exchange, in 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B). IEEE, 2017, pp. 1–6. 3.2

[11] P. Stanimirovi´c, J. Nikolov, I. Stanimirovi´c, A generalization of fibonacci and lucas matrices, Discrete applied mathematics, 156 (2008), pp. 2606–2619. 2.1, 2.1, 2.2

[12] P. Sundarayya, G. Vara Prasad, A public key cryptosystem using affine hill cipher under modulation of prime number, Journal of Information and Optimization Sciences, 40 (2019), pp. 919–930. 1

[13] P. K. Ray, G. K. Dila, B. K. Patel, Application of some recurrence relations to cryptography using finite state machine, International Journal of Computer Science and Electronics Engineering(IJCSEE), 2(4) (2014). 1

[14] S. Swain, C. Pratihary, P.K. Ray, Balancing and Lucas-Balancing Numbers and Their Application to Cryptography, Computer Engineering and Applications Journal, 5(1) (2016), pp.29-36. 1

[15] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE transactions on information theory, 31 (1985), pp. 469–472. 1, 3.1

[16] T. Koshy, Fibonacci and lucas numbers with applications, John Wiley & Sons, 2019. 1, 2

[17] W. Diffie, M. Hellman, New directions in cryptography, IEEE transactions on Information Theory, 22 (1976), pp. 644–654. 3.1

[18] Z. Zhang, Y. Zhang, The lucas matrix and some combinatorial identities, Indian Journal of Pure and Applied Mathematics, 38 (2007), p. 457. 2.1, 2