Journal of Mathematical Modeling
Vol. 11, No. 4, 2023, pp. 681–693. Research Article

JMM

A new public key cryptography using M_q matrix

Azadeh Ramezanpour Naseri[†], **Ahmad Abbasi**[†‡*], **Reza Ebrahimi Atani**[§]

[†]*Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Guilan, Rasht, Iran*
[‡]*Center of Excellence for Mathematical Modeling Optimization and Combinatorial Computing (MMOCC), University of Guilan, Rasht, Iran*
[§]*Department of Computer Engineering, University of Guilan, Rasht, Iran*
Email(s): azadehramezanpoor@gmail.com, aabbasi@guilan.ac.ir, rebrahimi@guilan.ac.ir

Abstract. We consider a new class of square Fibonacci $(q+1)\times(q+1)$-matrices in public key cryptography. This extends previous cryptography using generalized Fibonacci matrices. For a given integer q, a $(q+1)\times(q+1)$ binary matrix M_q is a matrix which nonzero entries are located either on the super diagonal or on the last row of the matrix. In this article, we have proposed a modified public key cryptography using such matrices as key in Hill cipher and key agreement for encryption-decryption of terms of M_q-matrix. In this scheme, instead of exchanging the whole key matrix, only a pair of numbers needed to be exchanged, which reduces the time complexity as well as the space complexity of the transmission and has a large key space.

Keywords: Cryptography, Hill cipher, key exchange Elgamal, Fibonacci sequence and M_q-matrix.
AMS Subject Classification 2010: 11T71, 11B39, 94A60.

1 Introduction

Information is one of the most valuable asset in the present-day world. The secured transmission of information is of prime importance. Cryptography is one of the methods to ensure confidentiality and integrity of the information. The Hill cipher was invented by Hill [4]. In classical cryptography, the Hill cipher is a poly-graphic substitution cipher, in which more than one letter can be encrypted at a time, based on linear algebra [8]. In the original Hill cipher, the massage sender encrypts $C = KP$, where C is a ciphertext matrix, P is any plaintext matrix and K is an invertible matrix (private key). Many researcher and papers tried to use Hill cipher algorithm to build a comprehensive cryptosystem, since Hill cipher has several advantages such as disguising letter frequencies of the plaintext, and its simplicity because of

[*]Corresponding author

Received: 1 March 2023 / Revised: 15 May 2023 / Accepted: 27 July 2023
DOI: 10.22124/JMM.2023.23982.2142

using multiplication of matrices and inversion for encryption and decryption and its high speed and high throughput [6]. Despite of speed the Hill cipher is no longer used due to the vulnerable against known plaintext attack because of its linearity [11]. For more terminology one can see [1, 5, 14].

In Recent research and development efforts, there are some studies on the security of Hill Cipher. Viswanath and Kumar [15] proposed a public key cryptosystem using Hill's cipher, in which the security of the system depends on the involvement of two digital signatures. Hasoun et al. [3] proposed a new approach of classical Hill cipher in public key cryptography, where method relies on the security of the RSA and involuntary key matrix. Hill cipher is vulnerable to a brute force attack because the Hill cipher key space is small [9] (The key space is the set of all possible keys, and its size is the number of possible keys). In this study, a novel technique of Hill cipher is proposed which is applied to the key matrix. So that instead of exchanging the whole key matrix, only a pair of numbers needed to be exchanged which reduces the time complexity as well as space complexity of the key transmission and has a large key space. Prasad and Mahato [10] have proposed a public key cryptosystem using generalized Fibonacci matrices. Zeriouh et al. [16], proposed the concept of key exchange between Alice and Bob using specially designed matrices. In this paper, we develop a public key cryptosystem using Hill cipher with M_q-matrices as a large keyspace for our proposed scheme that increases its efficiency. This method is quite robust and can be implemented.

This paper is organized as follows. In Section 2, we briefly introduce the Hill cipher. In Section 3 we give the matrix M_q by a new class of the Fibonacci sequence. Our proposed scheme is introduced in Section 4. In Section 5 we analyze the key space and we render the conclusion of the paper in Section 6 .

2 Hill cipher

One of the famous algorithms in cryptography based on the linear algebra is the Hill cipher algorithm. Hill cipher is the first polygraphic cipher. A polygraphic cipher is a cipher where the plaintext is divided into parts of adjacent letters of the same fixed length n, and then each such part is transformed into a different part of n letters. This polygraphic feature increased the speed and computations of the Hill cipher. Besides, it has some other advantages in data encryption, such as it resists the frequency of analysis attacks. The core of the Hill cipher is matrix multiplication [6]. Hill's encryption scheme takes n successive plaintext letters and substitutes them for n ciphertext letters. Here, we use matrix representation P for plaintext, K for the key matrix, and C for the ciphertext [11] as

$$P = [P_1, P_2, \ldots, P_m]^t, \quad K = \begin{pmatrix} K_{11} & K_{12} & \cdots & K_{1n} \\ K_{21} & K_{22} & \cdots & K_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ K_{n1} & K_{n2} & \cdots & K_{nn} \end{pmatrix}, \quad \text{and } C = [C_1, C_2, \ldots, C_m]^t,$$

where $P_i^{;}s$ and $C_i^{;}s$ are block matrices of size $1 \times n$. Thus, Hill Cipher scheme is described as following. For encryption, we set

$$C_i \equiv P_i K \pmod{p},$$

and for decryption, we consider

$$P_i \equiv C_i K^{-1} \pmod{p},$$

where p is a prime number and $\gcd(\det(K), p) = 1$.

3 The matrix M_q

The Fibonacci sequence is the sequence of integers F_n defined by

$$F_{n+2} = F_{n+1} + F_n \ \ , \ \ n \geq 0, \tag{1}$$

with the initial terms $F_0 = 0$, $F_1 = 1$ (see [7] for more details). The Fibonacci Q-matrix is defined as follows [2]

$$Q = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

From [12, 13], we know that the nth power of the Fibonacci Q-matrix is of the form

$$Q^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}.$$

The determinant of the Fibonacci Q-matrix is given by $\det(Q^n) = F_{n-1}F_{n+1} - F_n^2 = (-1)^n$.

Stakhov [12] introduced a new class of square matrices Q_p of the order $p+1$, where $p = 0, 1, 2, 3, \ldots$, which is a generalization of the Fibonacci Q-matrix

$$Q_p = \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}_{(p+1)\times(p+1)}.$$

He defined the Fibonacci p-numbers for $p = 0, 1, 2, 3, \ldots$, by the following way

$$F_p(n) = \begin{cases} F_p(n-1) + F_p(n-p-1), & n > p+1, \\ F_p(n+p+1) - F_p(n+p), & n \leq 0, \\ 1, & 1 \leq n \leq p+1. \end{cases}$$

He showed that the entries of Q_p-matrices may be obtained from the Fibonacci p-numbers by the following way,

$$Q_p = \begin{pmatrix} F_p(2) & F_p(1) & \ldots & F_p(3-p) & F_p(2-p) \\ F_p(2-p) & F_p(1-p) & \ldots & F_p(3-2p) & F_p(2-2p) \\ F_p(3-p) & F_p(2-p) & \ldots & F_p(4-2p) & F_p(3-2p) \\ \vdots & \vdots & & \vdots & \vdots \\ F_p(0) & F_p(-1) & \ldots & F_p(1-p) & F_p(-p) \\ F_p(1) & F_p(0) & \ldots & F_p(2-p) & F_p(1-p) \end{pmatrix}.$$

Stakhov [13] proved that for any $p = 0, 1, 2, 3, \dots$ and $n > 0$ one has

$$Q_p^n = \begin{pmatrix} F_p(n+1) & F_p(n) & \dots & F_p(n+2-p) & F_p(n+1-p) \\ F_p(n+1-p) & F_p(n-p) & \dots & F_p(n+2-2p) & F_p(n+1-2p) \\ F_p(n+2-p) & F_p(n+1-p) & \dots & F_p(n+3-2p) & F_p(n+2-2p) \\ \vdots & \vdots & & \vdots & \vdots \\ F_p(n-2) & F_p(n-3) & \dots & F_p(n-1-p) & F_p(n-2-p) \\ F_p(n-1) & F_p(n-2) & \dots & F_p(n-p) & F_p(n-1-p) \\ F_p(n) & F_p(n-1) & \dots & F_p(n+1-p) & F_p(n-p) \end{pmatrix}.$$

Therefore, Q_p^n satisfies the following properties [12]

(1) $Q_p^n Q_p^m = Q_p^{n+m}$,
(2) $Q_p^n = Q_p^{n-1} + Q_p^{n-p-1}$,
(3) $\det\ Q_p^n = (-1)^{pn} = (\det Q_p)^n$,

where $p = 0, 1, 2, 3, \dots$ and $n \in \mathbb{Z}$. Moreover, for the inverse of Q_p^n one may consider the following matrix

$$Q_p^{-n} = \begin{pmatrix} F_p(-n+1) & F_p(-n) & \dots & F_p(-n+1-p) \\ F_p(-n+1-p) & F_p(-n-p) & \dots & F_p(-n+1-2p) \\ F_p(-n+2-p) & F_p(-n+1-p) & \dots & F_p(-n+2-2p) \\ \vdots & \vdots & \vdots & \vdots \\ F_p(-n-2) & F_p(-n-3) & \dots & F_p(-n-2-p) \\ F_p(-n-1) & F_p(-n-2) & \dots & F_p(-n-1-p) \\ F_p(-n) & F_p(-n-1) & \dots & F_p(-n-p) \end{pmatrix}.$$

Now, we define a new class of $(q+1) \times (q+1)$-matrices called M_q, as

$$M_q = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \dots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \dots & 0 \\ 0 & \dots & \dots & \dots & 0 & 1 \\ 1 & 1 & \dots & \dots & \dots & 1 \end{pmatrix}_{(q+1)\times(q+1)} . \tag{2}$$

For $q = 1, \dots, 4$, $M_q's$ have, respectively, the following form

$$M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},\ M_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},\ M_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix},\ M_4 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Lemma 1. *Determinant of M_q is given by*

$$\det(M_q) = (-1)^q. \tag{3}$$

Proof. Clearly, one can see by induction on q that $\det(M_{q+1}) = -\det(M_q)$. So, the result comes from $\det(M_1) = -1$. □

Let us consider a representation for M_q as a generalization of (2), given by

$$M_q = \begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_{q-1} & a_q \\ a_q & a_{q+1} & \cdots & \cdots & a_{2q-1} & a_{2q} \\ \vdots & \ddots & \cdots & \cdots & \cdots & \vdots \\ \vdots & \ddots & \cdots & \cdots & \cdots & \vdots \\ a_{q^2-q} & a_{q^2-q+1} & \cdots & \cdots & a_{q^2-1} & a_{q^2} \\ a_{q^2} & a_{q^2+1} & \cdots & \cdots & a_{q^2+q-1} & a_{q^2+q} \end{pmatrix}_{(q+1)\times(q+1)}, \tag{4}$$

with $a_{kq+k+1} = 1$ for $0 \le k \le q-1$, $a_{q^2+k} = 1$ for $0 \le k \le q$ and $a_j = 0$, otherwise.

Now, we introduce a new sequence $\{a_n\}$ which generates (4).

Definition 1. For all integers $n \ge q^2 + q$, we introduce

$$a_n = a_{n-(q+1)q} + \cdots + a_{n-3q} + a_{n-2q} + a_{n-q}, \tag{5}$$

where $a_{kq+k+1} = 1$ for $0 \le k \le q-1$, $a_{q^2+k} = 1$ for $0 \le k \le q$ and $a_j = 0$, otherwise.

We consider the nth power of the M_q, M_q^n where its entries constructed by the sequence a_n defined by (5).

Example 1. Let us consider $q = 3$. By (1), the sequence a_n, for $n \ge 12$, has the following form

$$a_n = a_{n-12} + a_{n-9} + a_{n-6} + a_{n-3},$$

where $a_0, a_1, \ldots, a_{12}$ define matrix M_3 as the following form

$$M_3 = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_3 & a_4 & a_5 & a_6 \\ a_6 & a_7 & a_8 & a_9 \\ a_9 & a_{10} & a_{11} & a_{12} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Theorem 1. *For all integers $q = 0, 1, 2, \ldots$, $n \in \mathbb{Z}$, we have*

$$M_q^n = \begin{pmatrix} a_{q(n-1)} & a_{q(n-1)+1} & \cdots & \cdots & a_{qn-1} & a_{qn} \\ a_{qn} & a_{qn+1} & \cdots & \cdots & a_{q(n+1)-1} & a_{q(n+1)} \\ \vdots & \vdots & \cdots & \cdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \cdots & \cdots & \vdots \\ a_{q(n+q-2)} & a_{q(n+q-2)+1} & \cdots & \cdots & a_{q(n+p-1)-1} & a_{q(n+q-1)} \\ a_{q(n+q-1)} & a_{q(n+q-1)+1} & \cdots & \cdots & a_{q(n+q)-1} & a_{q(n+q)} \end{pmatrix}_{(q+1)\times(q+1)}, \tag{6}$$

where a_i's are the elements of the sequence a_n given in (5).

Proof. We prove the statement by induction on n. According to (4), it is obvious that the statement holds for $n=1$. Now, assuming the claim is true for $n-1$. We show that it is true for n. Considering $M_q^n = M_q M_q^{n-1}$, we show that $M_q X_j = Y_j$, where X_j, Y_j are the jth columns of M_q^{n-1} and M_q^n, respectively. We have

$$M_q.X_j = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & 0 & 1 \\ 1 & 1 & \dots & \dots & \dots & 1 \end{pmatrix} \begin{pmatrix} a_{q(n-2)+j-1} \\ a_{q(n-1)+j-1} \\ \vdots \\ \vdots \\ a_{q(n+q-3)+j-1} \\ a_{q(n+q-2)+j-1} \end{pmatrix} = \begin{pmatrix} a_{q(n-1)+j-1} \\ a_{qn+j-1} \\ \vdots \\ \vdots \\ a_{q(n+q-2)+j-1} \\ a_{q(n-2)+j-1} + \dots + a_{q(n+q-2)+j-1} \end{pmatrix}.$$

In the light of Definition 1, the last row of the column matrix $M_q X_j$ equals to $a_{q(n+q-1)+j-1}$. So, $M_q X_j = Y_j$ and we are done. □

In this scheme, we need M_q to be invertible. Thus, we consider the matrix M_q^n given with (6). Evidently, $\det(M_q^n) = (\det(M_q))^n$. Using (3), it is easy to prove the following proposition.

Proposition 1. *For given integers $q = 1,2,\dots$, we have $\det(M_q^n) = (-1)^{qn}$ where $n \in \mathbb{Z}^+$.*

For computing the inverse of M_q^n, we need to define a matrix M_{-q} and a sequence b_n. So, we define

$$M_{-q} := \begin{pmatrix} -1 & -1 & \dots & \dots & -1 & 1 \\ 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & 1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \dots & \dots & 1 & 0 & 0 \\ 0 & \dots & \dots & 0 & 1 & 0 \end{pmatrix}_{(q+1)\times(q+1)} . \tag{7}$$

We consider the another representation of M_{-q} as following

$$M_{-q} := \begin{pmatrix} b_{q^2+q} & b_{q^2+q-1} & \dots & \dots & b_{q^2+1} & b_{q^2} \\ b_{q^2} & b_{q^2-1} & \dots & \dots & b_{q^2-q+1} & b_{q^2-q} \\ \vdots & \ddots & \dots & \dots & \dots & \vdots \\ \vdots & \ddots & \dots & \dots & \dots & \vdots \\ b_{2q} & b_{2q-1} & \dots & \dots & b_{q+1} & b_q \\ b_q & b_{q-1} & \dots & \dots & b_1 & b_0 \end{pmatrix}_{(q+1)\times(q+1)} , \tag{8}$$

where $b_{q^2-kq-k} = 1$ for $0 \le k \le q-1$, $b_{q^2+k} = -1$ for $1 \le k \le q$ and $b_j = 0$, otherwise.

Definition 2. *For all integers $n \ge (q^2+q)$ we define*

$$b_n = b_{n-(q+1)q} - \dots - b_{n-3q} - a_{n-2q} - b_{n-q}, \tag{9}$$

where $b_{q^2-kq-k} = 1$ for $0 \le k \le q-1$, $b_{q^2+k} = -1$ for $1 \le k \le q$ and $b_j = 0$, otherwise.

Note that the terms of sequence b_n for $n = q^2+q, q^2, q^2-q, \ldots, q$ are the elements of the last column of the M_{-q}. From (2) and (7) one has

$$M_q M_{-q} = I_{q+1}. \tag{10}$$

So, the matrix M_{-q} is the inverse of M_q.

Corollary 1. The inverse of M_q^n is nth power of M_{-q}.

Proof. We have from equation (10) that $M_q M_{-q} = I_{q+1}$. Hence, $(M_q M_{-q})^n = I_{q+1}$, and so, $(M_q)^n (M_{-q})^n = I_{q+1}$. □

Theorem 2. *Let $q \in \mathbb{Z}^+$. Then for every integer $n \in \mathbb{Z}^+$, the inverse of M_q^n as M_{-q}^n which is given by*

$$M_{-q}^n = \begin{pmatrix} b_{q(n+q)} & b_{q(n+q)-1} & \cdots & \cdots & b_{q(n+q-1)+1} & b_{q(n+q-1)} \\ b_{q(n+q-1)} & b_{q(n+q-1)-1} & \cdots & \cdots & b_{q(n+q-2)+1} & b_{q(n+q-2)} \\ \vdots & \ddots & \cdots & \cdots & \cdots & \vdots \\ \vdots & \ddots & \cdots & \cdots & \cdots & \vdots \\ b_{q(n+1)} & b_{q(n+1)-1} & \cdots & \cdots & b_{qn+1} & b_{qn} \\ b_{qn} & b_{qn-1} & \cdots & \cdots & b_{q(n-1)+1} & b_{q(n-1)} \end{pmatrix}_{(q+1)\times(q+1)}, \tag{11}$$

where b_i's are elements of the sequence b_n in (9) and (8).

Proof. The proof clearly proceed by induction on n, similar the proof of Theorem 1. □

4 Proposed encryption scheme

In this section, we give a key exchange protocol (ElGamal Technique) and public key encryption scheme similar to Hill Cipher encryption scheme.

4.1 Key exchange protocol using Signature scheme

Elgamal announced a public-key scheme with digital signature based on discrete logarithm problem, closely related to the Diffie-Hellman technique [11]. The design of the Elgamal technique encryption is done by user's public key while decryption using user's private key. The key exchange protocol is defined as follows.

(i) **Domain parameters**: Let p be a prime number and α be a primitive root of p. Now choose a random integer X, such that $1 < X < p-1$, further compute $\beta = \alpha^X (\text{mod } p)$. Then make (p, α, β) as the public key and keep d as a secret key.

(ii) **Key exchange algorithm**: Alice first selects a random integer e such that $1 < e < p-1$ with $\gcd(e, p-1) = 1$ and then computes the signature $s = \alpha^e (\text{mod } p)$. (Note that this is the same as the computation of C for Elgamal encryption.) Also, Alice computes the secret key $\lambda = \beta^e (\text{mod } p)$. Thus

Primitive root: The exponent of α modulo p is the least positive integer k such that $\alpha^k = 1(\text{mod p})$. If the exponent of α modulo p is $\phi(p)$ then is said to be a primitive root of p.

Alice generates the parameters (λ, s) as an encryption key using Bob's public key (p, α, β), then encrypts the plaintext with the encryption key and sends (s, C) to Bob, where C is the corresponding cipher text.

(iii) **Key recover by Bob**: Now, Bob after receiving (s, C) from Alice, recovers secret key λ using their secret key X as,

$$s^X (\text{mod } p) = (\alpha^e)^X (\text{mod } p) = (\alpha^X)^e (\text{mod } p) = (\beta)^e (\text{mod } p) = \lambda. \tag{12}$$

Thus, Bob and Alice agree on the same parameters (λ, s) as the encryption key, i.e., the parameters (λ, s) as encryption key exchanged security and using these parameters, Bob can decrypts the C, and recovers the original plaintext P.

However, the consistency of the algorithms for encryption and decryption requires the next lemma. Using the fieldness of F_p one can easily state the following lemma.

Lemma 2. *Let p be a prime number. Then* $\det(M_q^n)(\text{mod } p) = \det(M_q^n(\text{mod } p))$.

4.2 Encryption algorithm

Now, to send message P to Bob, Alice first computes encryption key using Bob's public key (p, α, β) and encrypts his massage P as follows

1. Choosing a secret number e, such that $1 < e < p - 1$,
2. Computing Signature $s = \alpha^e (\text{mod } p)$ and secret key $\lambda = \beta^e (\text{mod } p)$,
3. Computing Key matrix as $K = M_\lambda^s (\text{mod } p)$,
4. Encryption of plain text and taking place as $C = Enc(P) : C_i = P_i K (\text{mod } p)$,
5. Sending (s, C) to Bob.

4.3 Decryption algorithm

After receiving (s, C) from Alice, Bob performs following operations to recover plaintext

1. Bob with his secret key X, calculates $\lambda = s^X (\text{mod } p)$,
2. computes key matrix $K = M_\lambda^s$,
3. decrypts the ciphertext as, $P = Dec(C) : P_i = C_i K^{-1} (\text{mod } p)$.

4.4 Numerical example

Considering $p = 47$, we encrypt the plaintext "**HELLO WORLD 2023**" with key matrix K using the proposed method. Assume, Alice wish to send a plaintext "**HELLO WORLD 2023**" to Bob. So for encryption, Alice needs the public key of Bob.

(Construction of Bob's Public key) Assume that $p = 47$ and Bob's private key is $X = 11$. Further, Bob chooses primitive root of p, say $\alpha = 19$.

Bob assigns $\alpha = 19$ and computes $\beta = \alpha^X (\text{mod } p) = 19^{11} (\text{mod } 47) = 29$. Thus, Bob's public key $\text{pk}(p, \alpha, \beta)$ is $\text{pk}(47, 19, 29)$ and secret key is $X = 11$. For encryption, Alice performs three steps.

Choosing e such that $1 < e < p - 1$, and let $e = 30$.

Calculating singnature, $s = \alpha^e = 19^{30} (\text{mod } 47) = 17$.

Calculating secret key $\lambda = \beta^e = 29^{30} (\text{mod } 47) = 6$.

Now, she constructs the key matrix $K = M_\lambda^s = M_6^{17}$:

$$K = M_6^{17} = \begin{pmatrix} a_{96} & a_{97} & a_{98} & a_{99} & a_{100} & a_{101} & a_{102} \\ a_{102} & a_{103} & a_{104} & a_{105} & a_{106} & a_{107} & a_{108} \\ a_{108} & a_{109} & a_{110} & a_{111} & a_{112} & a_{113} & a_{114} \\ a_{114} & a_{115} & a_{116} & a_{117} & a_{118} & a_{119} & a_{120} \\ a_{120} & a_{121} & a_{122} & a_{123} & a_{124} & a_{125} & a_{126} \\ a_{126} & a_{127} & a_{128} & a_{129} & a_{130} & a_{131} & a_{132} \\ a_{132} & a_{133} & a_{134} & a_{135} & a_{136} & a_{137} & a_{138} \end{pmatrix}$$

$$= \begin{pmatrix} 504 & 757 & 884 & 948 & 980 & 996 & 1004 \\ 1004 & 1508 & 1761 & 1888 & 1952 & 1984 & 2000 \\ 2000 & 3004 & 3508 & 3761 & 3888 & 3952 & 3984 \\ 3984 & 5984 & 6988 & 7492 & 7745 & 7872 & 7936 \\ 7936 & 11920 & 13920 & 14924 & 15428 & 15681 & 15808 \\ 15808 & 23744 & 27728 & 29728 & 30732 & 31236 & 31489 \\ 31489 & 47297 & 55233 & 59217 & 61217 & 62221 & 62725 \end{pmatrix},$$

and

$$K (\text{mod } 47) = \begin{pmatrix} 34 & 5 & 38 & 8 & 40 & 9 & 17 \\ 17 & 4 & 22 & 8 & 25 & 10 & 26 \\ 26 & 43 & 30 & 1 & 34 & 4 & 36 \\ 36 & 15 & 32 & 19 & 37 & 23 & 40 \\ 40 & 29 & 8 & 25 & 12 & 30 & 16 \\ 16 & 9 & 45 & 24 & 41 & 28 & 46 \\ 46 & 15 & 8 & 44 & 23 & 40 & 27 \end{pmatrix}.$$

Now, consider the plaintext **P=HELLO WORLD 2023**. The plaintext is divided into blocks as follows: $P_1 = [H\ E\ L\ L\ O\ W\ O] = [7\ 4\ 11\ 11\ 14\ 22\ 14]$, and $P_2 = [R\ L\ D\ 2\ 0\ 2\ 3] = [17\ 11\ 3\ 28\ 26\ 28\ 29]$.
Encryption: $C_i \leftarrow P_i K (\text{mod } p)$.

$$C_1 = P_1 K (\text{mod } 47) = [7\ 4\ 11\ 11\ 14\ 22\ 14] \begin{pmatrix} 34 & 5 & 38 & 8 & 40 & 9 & 17 \\ 17 & 4 & 22 & 8 & 25 & 10 & 26 \\ 26 & 43 & 30 & 1 & 34 & 4 & 36 \\ 36 & 15 & 32 & 19 & 37 & 23 & 40 \\ 40 & 29 & 8 & 25 & 12 & 30 & 16 \\ 16 & 9 & 45 & 24 & 41 & 28 & 46 \\ 46 & 15 & 8 & 44 & 23 & 40 & 27 \end{pmatrix} (\text{mod } 47)$$

$$= [6\ 46\ 41\ 16\ 15\ 22\ 41] \sim [G\ 20\ 15\ Q\ P\ W\ 15],$$

$$C_1 = P_1K(\text{mod } 47) = [7\ 4\ 11\ 11\ 14\ 22\ 14]\begin{pmatrix} 34 & 5 & 38 & 8 & 40 & 9 & 17 \\ 17 & 4 & 22 & 8 & 25 & 10 & 26 \\ 26 & 43 & 30 & 1 & 34 & 4 & 36 \\ 36 & 15 & 32 & 19 & 37 & 23 & 40 \\ 40 & 29 & 8 & 25 & 12 & 30 & 16 \\ 16 & 9 & 45 & 24 & 41 & 28 & 46 \\ 46 & 15 & 8 & 44 & 23 & 40 & 27 \end{pmatrix}(\text{mod } 47)$$

$$= [6\ 46\ 41\ 16\ 15\ 22\ 41] \sim [G\ 20\ 15\ Q\ P\ W\ 15],$$

$$C_2 = P_2K(\text{mod } 47) = [17\ 11\ 3\ 28\ 26\ 28\ 29]\begin{pmatrix} 34 & 5 & 38 & 8 & 40 & 9 & 17 \\ 17 & 4 & 22 & 8 & 25 & 10 & 26 \\ 26 & 43 & 30 & 1 & 34 & 4 & 36 \\ 36 & 15 & 32 & 19 & 37 & 23 & 40 \\ 40 & 29 & 8 & 25 & 12 & 30 & 16 \\ 16 & 9 & 45 & 24 & 41 & 28 & 46 \\ 46 & 15 & 8 & 44 & 23 & 40 & 27 \end{pmatrix}(\text{mod } 47)$$

$$= [20\ 4\ 2\ 20\ 37\ 24\ 13] \sim [U\ E\ C\ U\ 11\ Y\ N].$$

Thus, Alice encrypts the plaintext "**HELLO WORLD 2023**" to "**G2015QPW15UECU11YN**" and she sends the ciphertext C to Bob along with her signature, i.e., Alice sends $s = 17, C = (C_1, C_2)$ to Bob.

Decryption: On the other side Bob receives (s, C) from Aice. To construct the decryption key matrix K^*, Bob first recovers λ,

$$\lambda = s^X(\text{mod } 47) = 17^{11}(\text{mod } 47).$$

Thus, $K^* = M^{17}_{-6}$. Therefore,

$$K^* = M^{17}_{-6} = \begin{pmatrix} b_{138} & b_{137} & b_{136} & a_{135} & b_{134} & b_{133} & b_{132} \\ b_{132} & b_{131} & b_{130} & a_{129} & b_{128} & b_{127} & b_{126} \\ b_{126} & b_{125} & b_{124} & a_{123} & b_{122} & b_{121} & b_{120} \\ b_{120} & b_{119} & b_{118} & a_{117} & b_{116} & b_{115} & b_{114} \\ b_{114} & b_{113} & b_{112} & a_{111} & b_{110} & b_{109} & b_{108} \\ b_{108} & b_{107} & b_{106} & a_{105} & b_{104} & b_{103} & b_{102} \\ b_{102} & b_{101} & b_{100} & a_{199} & b_{198} & b_{197} & b_{196} \end{pmatrix},$$

and

$$K^*(\text{mod } 47) = \begin{pmatrix} -1 & -1 & -1 & -1 & 7 & -13 & 5 \\ 5 & 4 & 4 & 4 & 4 & 12 & -8 \\ -8 & -3 & -4 & -4 & -4 & -4 & 4 \\ 4 & -4 & 1 & 0 & 0 & 0 & 0 \\ 0 & 4 & -4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & -4 & 1 & 0 & 0 \\ 0 & 0 & 0 & 4 & -4 & 1 & 0 \end{pmatrix}.$$

Clearly, $K.K^* = 1 \pmod{47}$ (see Theorem 2). Thus the plaintext may be obtained by $P_i \leftarrow C_i K^* \pmod{p}$:

$$P_1 = C_1 K^* \pmod{47} = [6\ 46\ 41\ 16\ 15\ 22\ 41] \begin{pmatrix} -1 & -1 & -1 & -1 & 7 & -13 & 5 \\ 5 & 4 & 4 & 4 & 4 & 12 & -8 \\ -8 & -3 & -4 & -4 & -4 & -4 & 4 \\ 4 & -4 & 1 & 0 & 0 & 0 & 0 \\ 0 & 4 & -4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & -4 & 1 & 0 & 0 \\ 0 & 0 & 0 & 4 & -4 & 1 & 0 \end{pmatrix} \pmod{47}$$

$$= [7\ 4\ 11\ 11\ 14\ 22\ 14] \sim [H\ E\ L\ L\ O\ W\ O],$$

$$P_2 = C_2 K^* \pmod{47} = [20\ 4\ 2\ 20\ 37\ 24\ 13] \begin{pmatrix} -1 & -1 & -1 & -1 & 7 & -13 & 5 \\ 5 & 4 & 4 & 4 & 4 & 12 & -8 \\ -8 & -3 & -4 & -4 & -4 & -4 & 4 \\ 4 & -4 & 1 & 0 & 0 & 0 & 0 \\ 0 & 4 & -4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & -4 & 1 & 0 & 0 \\ 0 & 0 & 0 & 4 & -4 & 1 & 0 \end{pmatrix} \pmod{47}$$

$$= [17\ 11\ 3\ 28\ 26\ 28\ 29] \sim [R\ L\ D\ 2\ 0\ 2\ 3].$$

Thus, the plaintext "**HELLO WORLD 2023**" successfully received by Bob.

5 Security analysis

5.1 Brute force attack

In cryptography a brute force attack is a method of defeating a cryptographic scheme by trying a large number of passwords. In most of cases, a brute force attack typically means, testing all possible keys in order to recover the information used to produce a particular ciphertext.

In our proposed scheme, a new class of Fibonacci matrix and Elgamal technique have been considered as a key element of the system. One way for an adversary to break this scheme using brute force attack, is to consider all possible matrices. In the case of brute force attack, the adversary needs to calculate λ which is almost impossible (discrete logarithm problem), and the next challenge for the adversary is to identify the correct key matrix out of $|GL(\lambda)|$ matrices, where $GL(\lambda)$ represents general linear group [1], which consists of all invertible matrices of order $(\lambda+1)\times(\lambda+1)$ over F_p ($p > 26$ be a prime) and its order is given by

$$|GL_{\lambda+1}(F_p)| = (p^{\lambda+1} - p^{\lambda})(p^{\lambda+1} - p^{\lambda-1})\dots(p^{\lambda+1} - p)(p^{\lambda+1} - 1).$$

To examine strength of our system with the proposed key matrix M_λ^s over F_p, we are presenting a table of possible key over F_{47} based on general linear group.

Table 1: Some key matrix size over F_{47}

λ	s	Possible key spaces on $GL_{\lambda+1}(F_{47})$
1	$1,2,\cdots,s$	$\lvert GL_2(F_{47})\rvert = 4.667805\times 10^6$
2	$1,2,\cdots,s$	$\lvert GL_3(F_{47})\rvert = 1.11828\times 10^{15}$
3	$1,2,\cdots,s$	$\lvert GL_4(F_{47})\rvert = 9.6386152\times 10^{26}$
4	$1,2,\cdots,s$	$\lvert GL_5(F_{47})\rvert = 6.20734\times 10^{41}$
$\vdots$	$\vdots$	$\vdots$

6 Conclusion

In this paper, we have worked on a new class of square Fibonacci $(q+1)\times(q+1)$ matrices and their inverses. Also we have developed a public key cryptography using Hill cipher with M_{λ}^{s} under prime modulo, where M_{λ}^{s} is matrix of order $\lambda\times\lambda$.

Our proposed method enhances the security of the system, because it involves two digital signatures λ, s. As λ and s known only to Bob and Alice, it is not possible for any intruder to break this system. Our proposed method have advantages of large key space and computationally simple unlike the existing public key cryptosystem. The proposed system takes care of data integrity and authentications s and λ which is known only to Alice and Bob.

References

[1] D.S. Dummit, R.M. Foote, *Abstract Algebra*, Wiley Hoboken, 2004.

[2] H.W. Gould, *A history of the Fibonacci Q-matrix and a higher-dimensional problem*, Fibonacci Quart. **19** (1981) 250-257.

[3] R.K. Hasoun, S.F. Khlebus, H.K. Tayyeh, *A new approach of classical Hill cipher in public key cryptography*, Intern. J. Nonlinear Anal. Appl. **12** (2021) 1071-1082.

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

[5] F.E. Hoha, *Elementary Matrix Algebra*, New York: Macmillan Co. 1973.

[6] I.A. Ismail, M. Amin, H. Diab, *How to repair the Hill cipher*, J. Zhejiang Univ. Sci. **7** (2006) 2022-2030.

[7] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, New York, NY: John Wiley and Sons. 2001.

[8] S.S. M. Noor, N.M. Tahir, I.A. Yassin, A.M. Samad, *Creptosystem for secure Parking*, 2011 IEEE 7th International colloquium on signal Processing and its Applications.

[9] J. Overbey, W. Traves, J. Wojdylo, *On the key space of the Hill Cipher*, Cryptologia. **29** (2005) 59-72.

[10] K. Prasad, H. Mahato, *Cryptography using generalized Fibonacci matrices with Affine-Hill cipher*, J. Discrete Math. Sci. Cryptogr. **25** (2022) 2341-2352.

[11] W. Stallings, *Cryptography and Netwoek Security: Principles and Practice*, 7th Ed, Pearson Education Limited, 2017.

[12] A.P. Stakhov, *A generalizition of the Fibonacci Q-matrix*, Rep. Natl. Acad. Sci. Ukraine. **9** (1999) 46-49.

[13] A.P. Stakhov, *Fibonacci matrices, a generalization of the Cassini formula and a new coding theory*, Chaos Solitons Fractals **30** (2006) 56-66.

[14] D.R. Stinsonson, *Cryptography: Theory and Practice*, 3rd Ed. Chapman and Hall/CRC, Taylor & Francis Group, 2006.

[15] M. Viswanath, M.R. Kumar, *A public key cryptosystem using Hill's cipher*, J. Discrete Math. Sci. Cryptogr. **18** (2015) 129-138.

[16] M. Zeriouh, A. Chillali, A. Boua, *Cryptography based on the matrices*, Boletim Da Sociedade Paranaense De Matematica. **37** (2019) 75-83.