Electronic Journal of Mathematical Analysis and Applications
Vol. 11(2) July 2023, No. 4
ISSN: 2090-729X(online).
https://ejmaa.journals.ekb.eg/

CRYPTOGRAPHY UTILIZING THE AFFINE-HILL CIPHER AND EXTENDED GENERALIZED FIBONACCI MATRICES

V. BILLORE, N. PATEL

Abstract. We are aware that a major cryptosystem element plays a crucial part in maintaining the security and robustness of cryptography. Various researchers are focusing on creating new forms of cryptography and improving those that already exist using the principles of number theory and linear algebra. In this article, we have proposed an Extended generalized Fibonacci matrix (recursive matrix of higher order) having a relation with Extended generalized Fibonacci sequences and established some properties in addition to that usual matrix algebra. Further, we proposed a modified public key cryptography using these matrices as keys in Affine-Hill Cipher and key agreement for encryption-decryption with the combination of terms of Extended generalized Fibonacci sequences under prime modulo. This system has a large key space and reduces the time complexity as well as space complexity of the key transmission by only requiring the exchange of pair of numbers(parameters) as opposed to the entire key matrix.

Keywords: Affine Hill Cipher, Cryptography, Fibonacci Sequence & Matrix, Extended generalized Fibonacci Sequence & Matrix.
2020 Mathematics Subject Classification: 11T71, 11B37, 11B39, 11C20, 94A60, 14G50, 68P30.

1. Introduction

The theory of matrices has a wide range of unique characteristics, some of which are dependent on the way they were built, how their eigenvalues interact, and how they may be inverted. Several Scientific disciplines, as well as engineering and technology, employ matrices because of how they are built. One such field is cryptography [1, 11, 14, 15, 18], where the expansion of key spaces, the effectiveness of encryption-decryption and data storage are all greatly aided by matrix theory. It is widely known that recursive sequences are defined in terms of sums, differences or products (basic operation) on previous terms of related sequences. There is now a lot of study being done on the generalization of existing sequences for higher order as well as a generalization for arbitrary beginning values. While some authors produced extensions by examining the same connection but with other multipliers(constant/arbitrary functions as coefficients), some of these more recent advances and their applications may be found in [8, 9, 19].

2010 *Mathematics Subject Classification.* 11T71, 11B37, 11B39, 11C20, 94A60, 14G50, 68P30.
Key words and phrases. Affine Hill Cipher, Cryptography, Fibonacci Sequence & Matrix, Extended generalized Fibonacci Sequence & Matrix.
Submitted April 1, 2023.

We are aware that well-known identities of the Fibonacci sequences and the Lucas sequences [7] can be calculated using the recurrence relation $f_{\eta+2} = f_\eta + f_{\eta+1}, \quad \eta \geq 0$. The initial values of sequences are 0, 1, and 2, 1 respectively. Similarly, with initial values of 0,1,1 and 3,1,3 respectively, the Tribonacci sequences and Lucas sequences of order three are also given by the recurrence relation $f_{\eta+3} = f_\eta + f_{\eta+1} + f_{\eta+2}, \quad \eta \geq 0$. The following matrix representation [7] have been obtained, where $f_{\eta,\xi}$ denotes the ξ^{th} term of the sequence of order η and they correspond to the recursive sequence of order two and three mentioned above.

$$\begin{pmatrix} f_{2,\xi+1} & f_{2,\xi} \\ f_{2,\xi} & f_{2,\xi-1} \end{pmatrix}, \quad \begin{pmatrix} f_{3,\xi+2} & f_{3,\xi+1} + f_{3,\xi} & f_{3,\xi+1} \\ f_{3,\xi+1} & f_{3,\xi} + f_{3,\xi-1} & f_{3,\xi} \\ f_{3,\xi} & f_{3,\xi-1} + f_{3,\xi-2} & f_{3,\xi-1} \end{pmatrix}$$

We also know the generalization of Fibonacci sequence [12] of order θ is given by the recurrence relation $f_{\eta+\theta} = f_\eta + f_{\eta+1} + ... + f_{\eta+\theta-1}, \quad \eta \geq 0,\ \theta \in \mathbb{Z}^+$, with initial values $f_0 = f_1 = ... = f_{\theta-2} = 0,\ f_{\theta-1} = 1$. and the matrix representation [12] corresponding to above recursive sequence of θ^{th} order and there has been obtained as follows:

$$\begin{pmatrix} f_\theta & f_{\theta-1} + ... + f_0 & f_{\theta-1} + ... + f_1 & \cdots & f_{\theta-1} \\ f_{\theta-1} & f_{\theta-2} + ... + f_{-1} & f_{\theta-2} + ... + f_0 & \cdots & f_{\theta-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f_2 & f_1 + ... + f_{-\theta} & f_1 + ... + f_{1-\theta} & \cdots & f_1 \\ f_1 & f_0 + ... + f_{-\theta-1} & f_0 + ... + f_{-\theta} & \cdots & f_0 \end{pmatrix}$$

Another generalization of Fibonacci sequence [6] is given by the recurrence relation $f_\eta = af_{\eta-1} + bf_{\eta-2}, \quad \eta \geq 2$ with initial values 0, 1.

Laster Hill, a mathematician, created the Hill cipher in 1929. It is one of the polygraphic substitution cipher used in classical cryptography which is based on the residue system and linear algebra.

The idea of employing Hill's cipher for public key cryptography was put up by M.K. Viswanath,et al. [21]. They created the Hill's cipher system for public key cryptography utilising a rectangular matrix and they utilised the moorepenrose inverse(pseudo inverse) technique to compute the inverse key matrix. P. Sundarayya and G.V. Prasad [17] collaborated on the same article [21], and they proposed a solution that would use two or more digital signature to improve the security of the above system. By encrypting am m- length string to an n- length string ($n \geq m$) using affine transformation and polynomial transformation. Thilaka and Rajalakshmi [20] expanded the idea of the Hill cipher and increased its security.

In this paper, we are working on the generalization of Fibonacci sequence to higher order with different multipliers(constant/arbitrary functions as coefficient) called as extended generalized Fibonacci sequence. Recursive matrices have been constructed with entries derived from combination of terms of suggested sequences.Further, we apply these matrices to the Affine-Hill method and access the method's behaviour and strength.

This paper is organized as follows, the related work on the creation of recursive matrices and it's applications is introduced in section 1. In section 2, preliminaries on the cryptographic scheme, Elgamal technique and their mathematical formulation are studied. In section 3, we have established extended generalized Fibonacci sequences & matrices and discussed some remarkable properties. We presented a novel method for key exchange and encryption-decryption scheme with an example in section 4. Finally, we discussed the effectiveness of the suggested system in section 5 and then in section 6, we came to conclusion.

2. Preliminaries

Affine-Hill Cipher

The Affine-Hill Cipher is a polygraphic block cipher that converts blocks of size $\xi \geq 1$ of consecutive plaintext into ciphertext and vice versa, and is an equivalent to the Hill Cipher [14,15]. Assume that N is the plaintext, M is the key matrix (also known as the key) and Q is the associated ciphertext, each with a size of $1\times\xi$,$\xi\times\xi$, and $1\times\xi$, respectively. i.e

$$N = \begin{pmatrix} n_1 & n_2 & \cdots & n_n \end{pmatrix}, \ M = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1\xi} \\ m_{21} & m_{22} & \cdots & m_{2\xi} \\ \cdots & \cdots & \cdots & \cdots \\ m_{\xi 1} & m_{\xi 2} & \cdots & m_{\xi\xi} \end{pmatrix} \text{ and } Q = \begin{pmatrix} q_1 & q_2 & \cdots & q_n \end{pmatrix}$$

The Affine-Hill Cipher's method is defined as follows:

$$Enc(p) : q_i \equiv (n_i M + G) \quad (mod\ p) \tag{2.1}$$

$$Dec(C) : n_i \equiv (q_i - G)M^{-1} \quad (mod\ p) \tag{2.2}$$

where q_i, n_i are block vectors of size $1\times\xi$and G is a $1\times\xi$ row matrix, p is a prime integer that is larger than the variety of characters used in plaintext, while $Enc(P)$ & $Dec(C)$ stand for encryption and decryption methods, respectively.

2.1. **Algorithm for Key exchange(ELGAMAL Technique).** A public-key strategy based on discrete logarithms [3] and closely linked to the Deffie-Hellman method was suggested by T. Elgamal in 1984 [11,14,15]. The chosen prime p and the chosen primitive root of p serve as the global elements in the Elgamal approach. The Elgamal approach is built so that users' public keys are used for encryption and their private keys are used for decryption. Elgamal scheme is described as follows:

2.1.1. **Creation of Public key.** Let p be a prime number. choose a primitive root of p, let's say ρ and then a private key R such that $1 < R < \phi(p)$. Then, make $(p, \Re_1, \Re_2)$ the public key and keep R as the secret key by assigning $\Re_1 = \rho$ and $\Re_2 = \Re_1^R \ (modp)$.

2.1.2. **Key Swapping.** using the public key $(p, \Re_1, \Re_2)$, Alice creates η as shown below:

- **(i):** In order for $1 < \omega < \phi(p)$ to hold, choose a random integer ω.
- **(ii):** Find the signature using formula $\eta = \Re_1^\omega \ (mod\ p)$
- **(iii):** Make the secret key $\xi = \Re_2^\omega \ (mod\ p)$ calculations.
- **(iv):** Therefore, Alice can encrypt messages with their secret key ξ and transmit (η, Q) them once she gets access to Bob's public key.

2.1.3. **Key Recovery by Bob**. When Bob receive's (η, Q) from Alice, she uses their secret key R to find the secret key ξ as follows:

$$\begin{aligned} \xi &= \eta^R \pmod p \\ &\equiv (\Re_1^\omega)^R \pmod p \\ &\equiv (\Re_1^R)^\omega \pmod p \\ &\equiv (\Re_2)^\omega \pmod p \end{aligned} \tag{2.3}$$

As a result, Bob successfully receives the secret key ξ and using this secret key ξ, Bob will decrypt the ciphertext Q and get the original plaintext N.

3. Extended Generalized Fibonacci Sequences and Matrix Construction

The ξ^{th} order Extended generalized Fibonacci sequence is given by the following recurrence relation:

$$g_{a,b,\eta} = a^{\xi-1}g_{a,b,\eta-1}+a^{\xi-2}bg_{a,b,\eta-2}+\ldots+ab^{\xi-2}g_{a,b,\eta-\xi+1}+b^{\xi-1}g_{a,b,\eta-\xi} \qquad \eta \geq 0, \xi(\geq 2), a, b \in \mathbb{N} \tag{3.1}$$

with initial values $g_{a,b,0} = g_{a,b,1} = \ldots = g_{a,b,\xi-2} = 0$, $g_{a,b,\xi-1} = 1$.
Consider the corresponding $M_{a,b,\xi}$-matrix of order ξ, given by

$$M_{a,b,\xi} = \begin{pmatrix} a^{\xi-1} & a^{\xi-2}b & \ldots & ab^{\xi-2} & b^{\xi-1} \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}_{\xi\times\xi}$$

$$= \begin{pmatrix} g_{a,b,\xi} & a^{\xi-2}bg_{a,b,\xi-1} + a^{\xi-3}b^2g_{a,b,\xi-2} + \ldots + b^{\xi-1}g_{a,b,1} & a^{\xi-3}b^2g_{a,b,\xi-1} + a^{\xi-4}b^3g_{a,b,\xi-2} + \ldots + b^{\xi-1}g_{a,b,2} & \ldots & b^{\xi-1}g_{a,b,\xi-1} \\ g_{a,b,\xi-1} & a^{\xi-2}bg_{a,b,\xi-2} + a^{\xi-3}b^2g_{a,b,\xi-3} + \ldots + b^{\xi-1}g_{a,b,0} & a^{\xi-3}b^2g_{a,b,\xi-2} + a^{\xi-4}b^3g_{a,b,\xi-3} + \ldots + b^{\xi-1}g_{a,b,1} & \ldots & b^{\xi-1}g_{a,b,\xi-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{a,b,2} & a^{\xi-2}bg_{a,b,1} + a^{\xi-3}b^2g_{a,b,0} + \ldots + b^{\xi-1}g_{a,b,-\xi+3} & a^{\xi-3}b^2g_{a,b,1} + a^{\xi-4}b^3g_{a,b,0} + \ldots + b^{\xi-1}g_{a,b,-\xi+4} & \ldots & b^{\xi-1}g_{a,b,1} \\ g_{a,b,1} & a^{\xi-2}bg_{a,b,0} + a^{\xi-3}b^2g_{a,b,-1} + \ldots + b^{\xi-1}g_{a,b,-\xi+2} & a^{\xi-3}b^2g_{a,b,0} + a^{\xi-4}b^3g_{a,b,-1} + \ldots + b^{\xi-1}g_{a,b,-\xi+3} & \ldots & b^{\xi-1}g_{a,b,0} \end{pmatrix}$$

and using mathematical induction, it can be observed that

$$M^\eta_{a,b,\xi} = \begin{pmatrix} a^{\xi-1} & a^{\xi-2}b & \ldots & ab^{\xi-2} & b^{\xi-1} \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}^\eta$$

$$= \begin{pmatrix} g_{a,b,\eta+\xi-1} & a^{\xi-2}bg_{a,b,\eta+\xi-2} + a^{\xi-3}b^2g_{a,b,\eta+\xi-3} + \ldots + b^{\xi-1}g_{a,b,\eta} \\ g_{a,b,\eta+\xi-2} & a^{\xi-2}bg_{a,b,\eta+\xi-3} + a^{\xi-3}b^2g_{a,b,\eta+\xi-4} + \ldots + b^{\xi-1}g_{a,b,\eta-1} \\ \vdots & \vdots \\ g_{a,b,\eta+1} & a^{\xi-2}bg_{a,b,\eta} + a^{\xi-3}b^2g_{a,b,\eta-1} + \ldots + b^{\xi-1}g_{a,b,\eta-\xi+2} \\ g_{a,b,\eta} & a^{\xi-2}bg_{a,b,\eta-1} + a^{\xi-3}b^2g_{a,b,\eta-2} + \ldots + b^{\xi-1}g_{a,b,\eta-\xi+1} \end{pmatrix}$$

$$\begin{matrix} a^{\xi-3}b^2 g_{a,b,\eta+\xi-2} + a^{\xi-4}b^3 g_{a,b,\eta+\xi-3} + \ldots + b^{\xi-1} g_{a,b,\eta+1} & \ldots & b^{\xi-1} g_{a,b,\eta+\xi-2} \\ a^{\xi-3}b^2 g_{a,b,\eta+\xi-3} + a^{\xi-4}b^3 g_{a,b,\eta+\xi-4} + \ldots + b^{\xi-1} g_{a,b,\eta} & \ldots & b^{\xi-1} g_{a,b,\eta+\xi-3} \\ \vdots & \ddots & \vdots \\ a^{\xi-3}b^2 g_{a,b,\eta} + a^{\xi-4}b^3 g_{a,b,\eta-1} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+3} & \ldots & b^{\xi-1} g_{a,b,\eta} \\ a^{\xi-3}b^2 g_{a,b,\eta-1} + a^{\xi-4}b^3 g_{a,b,\eta-2} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+2} & \ldots & b^{\xi-1} g_{a,b,\eta-1} \end{matrix}\Bigg) \tag{3.2}$$

Remark 1. *Let $M^{\eta}_{a,b,\xi}$ is Extended generalized Fibonacci matrix of order $\xi \times \xi$, then we observed that $M^{\eta}_{a,b,\xi}.M^{1}_{a,b,\xi} = M^{\eta+1}_{a,b,\xi}$ as*
$M^{\eta}_{a,b,\xi}.M^{1}_{a,b,\xi}$

$$= \Bigg(\begin{matrix} g_{a,b,\eta+\xi-1} & a^{\xi-2}b g_{a,b,\eta+\xi-2} + a^{\xi-3}b^2 g_{a,b,\eta+\xi-3} + \ldots + b^{\xi-1} g_{a,b,\eta} \\ g_{a,b,\eta+\xi-2} & a^{\xi-2}b g_{a,b,\eta+\xi-3} + a^{\xi-3}b^2 g_{a,b,\eta+\xi-4} + \ldots + b^{\xi-1} g_{a,b,\eta-1} \\ \vdots & \vdots \\ g_{a,b,\eta+1} & a^{\xi-2}b g_{a,b,\eta} + a^{\xi-3}b^2 g_{a,b,\eta-1} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+2} \\ g_{a,b,\eta} & a^{\xi-2}b g_{a,b,\eta-1} + a^{\xi-3}b^2 g_{a,b,\eta-2} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+1} \end{matrix}$$

$$\begin{matrix} a^{\xi-3}b^2 g_{a,b,\eta+\xi-2} + a^{\xi-4}b^3 g_{a,b,\eta+\xi-3} + \ldots + b^{\xi-1} g_{a,b,\eta+1} & \ldots & b^{\xi-1} g_{a,b,\eta+\xi-2} \\ a^{\xi-3}b^2 g_{a,b,\eta+\xi-3} + a^{\xi-4}b^3 g_{a,b,\eta+\xi-4} + \ldots + b^{\xi-1} g_{a,b,\eta} & \ldots & b^{\xi-1} g_{a,b,\eta+\xi-3} \\ \vdots & \ddots & \vdots \\ a^{\xi-3}b^2 g_{a,b,\eta} + a^{\xi-4}b^3 g_{a,b,\eta-1} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+3} & \ldots & b^{\xi-1} g_{a,b,\eta} \\ a^{\xi-3}b^2 g_{a,b,\eta-1} + a^{\xi-4}b^3 g_{a,b,\eta-2} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+2} & \ldots & b^{\xi-1} g_{a,b,\eta-1} \end{matrix}\Bigg) \times$$

$$\begin{pmatrix} a^{\xi-1} & a^{\xi-2}b & \ldots & ab^{\xi-2} & b^{\xi-1} \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

entries of first column can be reduces using (3.1)*,which gives*

$$= \Bigg(\begin{matrix} g_{a,b,\eta+\xi} & a^{\xi-2}b g_{a,b,\eta+\xi-1} + a^{\xi-3}b^2 g_{a,b,\eta+\xi-2} + \ldots + b^{\xi-1} g_{a,b,\eta+1} \\ g_{a,b,\eta+\xi-1} & a^{\xi-2}b g_{a,b,\eta+\xi-2} + a^{\xi-3}b^2 g_{a,b,\eta+\xi-3} + \ldots + b^{\xi-1} g_{a,b,\eta} \\ \vdots & \vdots \\ g_{a,b,\eta+2} & a^{\xi-2}b g_{a,b,\eta+1} + a^{\xi-3}b^2 g_{a,b,\eta} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+3} \\ g_{a,b,\eta+1} & a^{\xi-2}b g_{a,b,\eta} + a^{\xi-3}b^2 g_{a,b,\eta-1} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+2} \end{matrix}$$

$$\begin{matrix} a^{\xi-3}b^2 g_{a,b,\eta+\xi-1} + a^{\xi-4}b^3 g_{a,b,\eta+\xi-2} + \ldots + b^{\xi-1} g_{a,b,\eta+2} & \ldots & b^{\xi-1} g_{a,b,\eta+\xi-1} \\ a^{\xi-3}b^2 g_{a,b,\eta+\xi-2} + a^{\xi-4}b^3 g_{a,b,\eta+\xi-3} + \ldots + b^{\xi-1} g_{a,b,\eta+1} & \ldots & b^{\xi-1} g_{a,b,\eta+\xi-2} \\ \vdots & \ddots & \vdots \\ a^{\xi-3}b^2 g_{a,b,\eta+1} + a^{\xi-4}b^3 g_{a,b,\eta} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+4} & \ldots & b^{\xi-1} g_{a,b,\eta+1} \\ a^{\xi-3}b^2 g_{a,b,\eta} + a^{\xi-4}b^3 g_{a,b,\eta-1} + \ldots + b^{\xi-1} g_{a,b,\eta-\xi+3} & \ldots & b^{\xi-1} g_{a,b,\eta} \end{matrix}\Bigg)$$

$= M^{\eta+1}_{a.b,\xi}$

Using the recurrence relation (3.1)*, we can also generalize the ξ^{th} order negative extended generalized Fibonacci sequences.*

Lemma 3.1. *Let p be prime and M is Extended generalized Fibonacci matrix, then*

$$det(M)(mod\ p) = det(M \quad (mod\ p))$$

Lemma 3.2. *Let $M^{\eta}_{a,b,\xi}$ is extended generalized Fibonacci matrix of order $\xi \times \xi$, then*

$$\begin{aligned} & det(M_{a,b,\xi}) = (-b)^{\xi-1} \qquad (\text{here} \quad \mathrm{M_{a,b,\xi} = M^1_{a,b,\xi}}) \\ \text{Thus,} \qquad & \det(\mathrm{M}^{\eta}_{\mathrm{a,b,\xi}}) = [(-b)^{\xi-1}]^{\eta} \\ & \qquad\qquad = (-b)^{\eta(\xi-1)} \end{aligned}$$

Theorem 3.1. *(Existence of Inverse of Extended generalized Fibonacci Matrix). Let $\xi(\geq 2), a, b \in \mathbb{N}$, then for every integer $\eta \in \mathbb{Z}$, the inverse of extended generalized Fibonacci matric$M^{\eta}_{a,,b,\xi}$ is given by $M^{-\eta}_{a,,b,\xi}$ as defined in equation* (3.2).

Proof. We shall prove existence by mathematical induction on η. Since, by the definition of $M^{\eta}_{a,,b,\xi}$(3.2), we have

$$M^{-1}_{a,,b,\xi} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ \frac{1}{b^{\xi-1}} & \frac{-a^{\xi-1}}{b^{\xi-1}} & \frac{-a^{\xi-2}}{b^{\xi-2}} & \dots & \frac{-a}{b} \end{pmatrix}_{\xi\times\xi}$$

and

$$M^{-\eta}_{a,,b,\xi} = \left(\begin{matrix} g_{a,b,-\eta+\xi-1} & a^{\xi-2}bg_{a,b,-\eta+\xi-2} + a^{\xi-3}b^2 g_{a,b,-\eta+\xi-3} + \dots + b^{\xi-1}g_{a,b,-\eta} \\ g_{a,b,-\eta+\xi-2} & a^{\xi-2}bg_{a,b,-\eta+\xi-3} + a^{\xi-3}b^2 g_{a,b,-\eta+\xi-4} + \dots + b^{\xi-1}g_{a,b,-\eta-1} \\ \vdots & \vdots \\ g_{a,b,-\eta+1} & a^{\xi-2}bg_{a,b,-\eta} + a^{\xi-3}b^2 g_{a,b,-\eta-1} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+2} \\ g_{a,b,-\eta} & a^{\xi-2}bg_{a,b,-\eta-1} + a^{\xi-3}b^2 g_{a,b,-\eta-2} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+1} \end{matrix}\right.$$

$$\left.\begin{matrix} a^{\xi-3}b^2 g_{a,b,-\eta+\xi-2} + a^{\xi-4}b^3 g_{a,b,-\eta+\xi-3} + \dots + b^{\xi-1}g_{a,b,-\eta+1} & \dots & b^{\xi-1}g_{a,b,-\eta+\xi-2} \\ a^{\xi-3}b^2 g_{a,b,-\eta+\xi-3} + a^{\xi-4}b^3 g_{a,b,-\eta+\xi-4} + \dots + b^{\xi-1}g_{a,b,-\eta} & \dots & b^{\xi-1}g_{a,b,-\eta+\xi-3} \\ \vdots & \ddots & \vdots \\ a^{\xi-3}b^2 g_{a,b,-\eta} + a^{\xi-4}b^3 g_{a,b,-\eta-1} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+3} & \dots & b^{\xi-1}g_{a,b,-\eta} \\ a^{\xi-3}b^2 g_{a,b,-\eta-1} + a^{\xi-4}b^3 g_{a,b,-\eta-2} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+2} & \dots & b^{\xi-1}g_{a,b,-\eta-1} \end{matrix}\right) \tag{3.3}$$

Now, for $\eta = 1$

$$M^{1}_{a,b,\xi}M^{-1}_{a,b,\xi} = \begin{pmatrix} a^{\xi-1} & a^{\xi-2}b & \dots & ab^{\xi-2} & b^{\xi-1} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ \frac{1}{b^{\xi-1}} & \frac{-a^{\xi-1}}{b^{\xi-1}} & \frac{-a^{\xi-2}}{b^{\xi-2}} & \dots & \frac{-a}{b} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}_{\xi\times\xi} = I_{\xi} \tag{3.4}$$

Since, we have $M^{-1}_{a,b,\xi}M^{-\eta}_{a,b,\xi} =$

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ \frac{1}{b^{\xi-1}} & \frac{-a^{\xi-1}}{b^{\xi-1}} & \frac{-a^{\xi-2}}{b^{\xi-2}} & \dots & \frac{-a}{b} \end{pmatrix} \times$$

$$\begin{pmatrix} g_{a,b,-\eta+\xi-1} & a^{\xi-2}bg_{a,b,-\eta+\xi-2} + a^{\xi-3}b^2 g_{a,b,-\eta+\xi-3} + \dots + b^{\xi-1}g_{a,b,-\eta} & a^{\xi-3}b^2 g_{a,b,-\eta+\xi-2} + a^{\xi-4}b^3 g_{a,b,-\eta+\xi-3} + \dots + b^{\xi-1}g_{a,b,-\eta+1} & \dots & b^{\xi-1}g_{a,b,-\eta+\xi-2} \\ g_{a,b,-\eta+\xi-2} & a^{\xi-2}bg_{a,b,-\eta+\xi-3} + a^{\xi-3}b^2 g_{a,b,-\eta+\xi-4} + \dots + b^{\xi-1}g_{a,b,-\eta-1} & a^{\xi-3}b^2 g_{a,b,-\eta+\xi-3} + a^{\xi-4}b^3 g_{a,b,-\eta+\xi-4} + \dots + b^{\xi-1}g_{a,b,-\eta} & \dots & b^{\xi-1}g_{a,b,-\eta+\xi-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{a,b,-\eta+1} & a^{\xi-2}bg_{a,b,-\eta} + a^{\xi-3}b^2 g_{a,b,-\eta-1} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+2} & a^{\xi-3}b^2 g_{a,b,-\eta} + a^{\xi-4}b^3 g_{a,b,-\eta-1} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+3} & \dots & b^{\xi-1}g_{a,b,-\eta} \\ g_{a,b,-\eta} & a^{\xi-2}bg_{a,b,-\eta-1} + a^{\xi-3}b^2 g_{a,b,-\eta-2} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+1} & a^{\xi-3}b^2 g_{a,b,-\eta-1} + a^{\xi-4}b^3 g_{a,b,-\eta-2} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+2} & \dots & b^{\xi-1}g_{a,b,-\eta-1} \end{pmatrix}$$

$$= \begin{pmatrix} g_{a,b,-\eta+\xi-2} & a^{\xi-2}bg_{a,b,-\eta+\xi-3} + a^{\xi-3}b^2 g_{a,b,-\eta+\xi-4} + \dots + b^{\xi-1}g_{a,b,-\eta-1} & a^{\xi-3}b^2 g_{a,b,-\eta+\xi-3} + a^{\xi-4}b^3 g_{a,b,-\eta+\xi-4} + \dots + b^{\xi-1}g_{a,b,-\eta} & \dots & b^{\xi-1}g_{a,b,-\eta+\xi-3} \\ g_{a,b,-\eta+\xi-3} & a^{\xi-2}bg_{a,b,-\eta+\xi-4} + a^{\xi-3}b^2 g_{a,b,-\eta+\xi-5} + \dots + b^{\xi-1}g_{a,b,-\eta-2} & a^{\xi-3}b^2 g_{a,b,-\eta+\xi-4} + a^{\xi-4}b^3 g_{a,b,-\eta+\xi-5} + \dots + b^{\xi-1}g_{a,b,-\eta-1} & \dots & b^{\xi-1}g_{a,b,-\eta+\xi-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{a,b,-\eta} & a^{\xi-2}bg_{a,b,-\eta-1} + a^{\xi-3}b^2 g_{a,b,-\eta-2} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+1} & a^{\xi-3}b^2 g_{a,b,-\eta-1} + a^{\xi-4}b^3 g_{a,b,-\eta-2} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+2} & \dots & b^{\xi-1}g_{a,b,-\eta-1} \\ g_{a,b,-\eta-1} & a^{\xi-2}bg_{a,b,-\eta-2} + a^{\xi-3}b^2 g_{a,b,-\eta-3} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi} & a^{\xi-3}b^2 g_{a,b,-\eta-2} + a^{\xi-4}b^3 g_{a,b,-\eta-3} + \dots + b^{\xi-1}g_{a,b,-\eta-\xi+1} & \dots & b^{\xi-1}g_{a,b,-\eta-2} \end{pmatrix}$$

$= M_{a,b,\xi}^{-(\eta+1)}$

Now, assume that the result holds for $\eta = m$, i.e.

$$M_{a,b,\xi}^{m}.M_{a,b,\xi}^{-m} = I_\xi \tag{3.5}$$

Thus, for $\eta = m + 1$, we have,

$$\begin{aligned} M_{a,b,\xi}^{(m+1)}.M_{a,b,\xi}^{-(m+1)} &= M_{a,b,\xi}^{m}.M_{a,b,\xi}^{1}.M_{a,b,\xi}^{-1}.M_{a,b,\xi}^{-m} \\ &= M_{a,b,\xi}^{m}.I_\xi.M_{a,b,\xi}^{-m} \qquad \text{Using equation(3.4)} \\ &= M_{a,b,\xi}^{m}.M_{a,b,\xi}^{-m} \qquad \text{Using equation(3.5)} \\ &= I_\xi \end{aligned}$$

Hence, proved. □

4. Encryption Scheme & Algorithm

Assume that the receiver (Bob) constructed the components of their public key $pk(p, \Re_1, \Re_2)$ with the aid of their private key R. The secret key ξ will now be determined using this public key (see, 2.1). After receiving the encrypted message with the signature from Alice, Bob further gets the secret key ξ, and after doing some calculations, recovers the plain text (see, section 2). The methodology is outlined in the next algorithm.

4.1. **Algorithm. Encryption Algorithm(sender have access to $pk(p, \Re_1, \Re_2)$):**

(1) Alice choose secret number ω, such that $1 < \omega < \phi(p)$.
(2) **Signature:** $\eta \leftarrow \Re_1^{\omega} \pmod p$.
(3) **Secret key:** $\xi \leftarrow \Re_2^{\omega} \pmod p$.
(4) **Key matrix:** $V \leftarrow M_{a,b,\xi}^{\eta}$, where $M_{a,b,\xi}$ is Extended generalized Fibonacci matrix with choosing the value of a, b of order $\xi \times \xi$.
(5) Choose shift vector G of order $1 \times \xi$.
(6) **Encryption:** $Q \equiv Enc(p) : q_i \leftarrow (n_i V + G) \quad (mod\ p)$.
(7) transmit (Q, G, η, a, b).

Decryption Algorithm: After receiving (Q, G, η, a, b)

(1) **Secret key:** $\xi \leftarrow \eta^R \pmod p$, where R is Bob Secret key.
(2) **Key Matrix:** $V^* \leftarrow M_{a,b,\xi}^{-\eta}$ with the help of signature key η, a, b.
(3) **Decryption:** $N \equiv Dec(c) : n_i \leftarrow (q_i - g)V^* \pmod p$.
(4) Plaintext (P) recovered.

4.2. **Example.**

Example 1. *Assume Alice wants to communicate with Bob. Assume that $p = 37$ is a prime number. Establish Bob's communication secret key and public key.*
Solution. First, Bob selects an integer R such that $1 < R < \phi(37)$, let's assume $R = 11$. $Z = \{2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35\}$ gives the set of primitive roots of 37. Now Bob chooses the primitive root to say $\rho = 2$ from Z. After setting up the public key, Bob now assign $\Re_1 = 2, \Re_2 = \Re_1^R \ (mod\ \ p) \equiv 2^{11} \pmod{37} \equiv 13$. Consequently, the public key $pk(p, \Re_1, \Re_2)$ for Bob and Alice is $pk(37, 2, 13)$. and Secret key is $sk(11)$. Now using $pk(37, 2, 13)$ anyone can send a message to Bob. (explained in the next example).

Example 2. *(Encryption-Decryption). Suppose plaintext be SUMAN2022, public key is $pk(37, 2, 13)$ and shifting vector G is [11,07,05].*
Solution. Let us consider alphabets defined as follows for letters from A-Z equivalent to 00-25, digits 0-9 are that to 26-35 and 36 for blank space/white space. Therefore, the numerical values equivalent to "SUMAN2022" is [18,20,12,00,13,28,26,28,28].
Now according to the algorithm (4.1),
Alice first choose an integer ω such that $1 < \omega < \phi(37)$, say $\omega = 22$.
Calculate Signature as $\eta = \Re_1^{\omega} = 2^{22} \pmod{37} \equiv 21$.
and Secret key $\xi = \Re_2^{\omega} = 13^{22} \pmod{37} \equiv 3$.
Now, construction the key matrix V using above data and assuming $a = 2, b = 2$ with help of Extended generalized Fibonacci matrix $M_{a,b,\xi}^{\eta}$ for encryption is given by

$$V = M_{2,2,3}^{21} = \begin{pmatrix} g_{2,2,23} & 4g_{2,2,22} + 4g_{2,2,21} & 4g_{2,2,22} \\ g_{2,2,22} & 4g_{2,2,21} + 4g_{2,2,20} & 4g_{2,2,21} \\ g_{2,2,21} & 4g_{2,2,20} + 4g_{2,2,19} & 4g_{2,2,20} \end{pmatrix} \pmod{37}$$
$$= \begin{pmatrix} 338586089570304 & 327536380411904 & 272648440315904 \\ 68162110078976 & 65937649254400 & 54887940096000 \\ 13721985024000 & 13274169982976 & 11049709158400 \end{pmatrix} \pmod{37}$$
$$= \begin{pmatrix} 0 & 5 & 26 \\ 25 & 11 & 16 \\ 4 & 9 & 32 \end{pmatrix}$$

which is obtained by substituting the values of corresponding terms of the Extended generalized Fibonacci sequence for $\xi = 3, a = 2$ and $b = 2$ as given in the table

index(η)	...	-1	0	1	2	3	4	...	19	20	21	22	23	...
$g_{2,2,\eta}$	...	$\frac{1}{4}$	*0*	*0*	*1*	4	20	...	556115206144	2762427289600	1372198502400	68962110078976	338586089570304	...

Now, divide the plaintext ***SUMAN2022*** *in blocks of size $1 \times \xi$ as follows:*
$n_1 = [S\ U\ M] = [18\ 20\ 21]$, $n_2 = [A\ N\ 2] = [00\ 13\ 28]$, $n_3 = [0\ 2\ 2] = [26\ 28\ 28]$.
Encryption: $q_i \leftarrow (n_i V + G) \pmod{37}$,

$$\begin{aligned} q_1 = (n_1V + G) &\equiv \left([18\ 20\ 21] \begin{pmatrix} 00 & 05 & 26 \\ 25 & 11 & 16 \\ 04 & 09 & 32 \end{pmatrix} + [11\ 07\ 05] \right) \pmod{37} \\ &\equiv [04\ 18\ 30] \sim (E\ S\ 4) \\ q_2 = (n_2V + G) &\equiv \left([00\ 13\ 28] \begin{pmatrix} 00 & 05 & 26 \\ 25 & 11 & 16 \\ 04 & 09 & 32 \end{pmatrix} + [11\ 07\ 05] \right) \pmod{37} \\ &\equiv [04\ 32\ 36] \sim (E\ 6\ \square) \\ q_3 = (n_3V + G) &\equiv \left([26\ 28\ 28] \begin{pmatrix} 00 & 05 & 26 \\ 25 & 11 & 16 \\ 04 & 09 & 32 \end{pmatrix} + [11\ 07\ 05] \right) \pmod{37} \\ &\equiv [09\ 31\ 27] \sim (J\ 5\ 1) \end{aligned}$$

Thus, Alice encrypted the plaintext ***SUMAN2022*** *to* ***ES4E6□J51****. and sent it to Bob along with her signature i.e. Alice send* $\{\ \eta = 21, a = 2, b = 2, G = [11\ 07\ 05], Q = q_1q_2q_3\}$ *to Bob.* ***Decryption:*** *After receiving ciphertext C along with signature (η, a, b, G). Bob will calculate the decryption key V^* with the help of their secret key R, which is given as :*

$$\xi = \eta^R \pmod{37} = 21^{11} \pmod{37} \equiv 3$$

Thus

$$\begin{aligned} V^* &= M_{2,2,3}^{-21} \pmod{37} \\ &= \begin{pmatrix} \frac{9265}{16384} & \frac{-2627}{2048} & \frac{-33275}{4096} \\ \frac{-33275}{16384} & \frac{142725}{16384} & \frac{28021}{4096} \\ \frac{28021}{16384} & \frac{-145359}{16384} & \frac{30641}{16384} \end{pmatrix} \pmod{37} \\ &= \begin{pmatrix} 31 & 00 & 28 \\ 07 & 03 & 09 \\ 30 & 35 & 31 \end{pmatrix}. \end{aligned}$$

Clearly, $VV^* = I \pmod{37}$.
Hence, Decryption takes place as $n_i \leftarrow (q_i - G).V^* \pmod{37}$.

$$n_1 = (q_1 - G).V^* = ([04\ 18\ 13] - [11\ 07\ 05]) \begin{pmatrix} 31 & 00 & 28 \\ 07 & 03 & 09 \\ 30 & 35 & 31 \end{pmatrix} \pmod{37}$$

$$\equiv [18\ 20\ 12] \sim (S\ U\ M)$$

$$n_2 = (q_2 - G).V^* = ([04\ 32\ 36] - [11\ 07\ 05]) \begin{pmatrix} 31 & 00 & 28 \\ 07 & 03 & 09 \\ 30 & 35 & 31 \end{pmatrix} \pmod{37}$$

$$\equiv [0\ 13\ 28] \sim (A\ N\ 2)$$

$$n_3 = (q_3 - G).V^* = ([09\ 31\ 27] - [11\ 07\ 05]) \begin{pmatrix} 31 & 00 & 28 \\ 07 & 03 & 09 \\ 30 & 35 & 31 \end{pmatrix} \pmod{37}$$

$$\equiv [26\ 28\ 28] \sim (0\ 2\ 2)$$

Thus, Bob recovered plaintext ***SUMAN2022*** *sent by Alice successfully.*

5. Strength Analysis

In our proposed scheme, the Extended generalized Fibonacci matrix and Elgamal technique have been considered a key element of the system, and the decryption matrix is set up as $M^{-\eta}_{a,b,\xi}$ constructed with combinations of terms of Extended generalized Fibonacci sequences. For authorized parties building key matrices is simple since they both know the value of ξ, η, a, b, but an adversary finding ξ, η, a, b is exceedingly challenging because they must solve a discrete logarithm problem [3]. Further, matrix building decreases the time and space complexity of key generation and inverse computation by relying just on four components(ξ, η, a, b). One of the widely used techniques in the context of assaults based on public data is the brute force attack [11,14,15], which has been covered here. The opponent must compute n in a brute force assault, which is nearly impossible(discrete logarithm problem) and the next task for the adversary is to choose the right key matrix from a set of $|GL(\xi)|$ matrices, where $|GL(\xi)|$ represent general linear group [2] of order n and defined by

$$|GL_\xi F(p)| = (p^\xi - p^{\xi-1})(p^\xi - p^{\xi-2})(p^\xi - p^{\xi-3}) \dots (p^\xi - p^1)(p^\xi - 1) \tag{5.1}$$

It is obvious from equation (5.1) that security for Extended generalized Fibonacci matrices $M^{\eta}_{a,b,\xi}$ completely depends on ξ and not η, a, b. As a result, even while the adversary is aware of η, a, b, it does not undermine the security. For instance, consider $p = 37$ and $\xi = 50$, then by equation (5.1) total number of potential key space over F_{37} is almost 3.105×10^{3920} which is too huge. Additionally, the key space expands exponentially as ξ and/or prime p increases.

6. Conclusion

In this article, we have first proposed an Extended generalized Fibonacci sequence with initial conditions. Further, we have developed a recursive matrix $M^{\eta}_{a,b,\xi}$ whose entries are constructed from a linear combination of Extended generalized Fibonacci sequences and investigated some properties. Because inverse is required, the Field is considered an important component. In our situation, we have taken

into consideration Extended generalized Fibonacci matrices, which do not constitute a multiplicative group but ensure the presence of an inverse matrix for each $M^{\eta}_{a,b,\xi}$ for every $(\eta \geq 2) \in \mathbb{N}$ i.e. we have proven that for every integer η, we have matrix $V^* = M^{-\eta}_{a,b,\xi}$ such that $V^* M^{\eta}_{a,b,\xi} = M^{\eta}_{a,b,\xi} V^* = I_n$.
Additionally, we have proposed a modified public key cryptography using Affine-Hill Cipher & Elgamal Signature Scheme with Extended generalized Fibonacci matrices and show the implementation of Extended generalized Fibonacci matrices as a key matrix.
Our proposed method strengthen the security of the system which has five digital signature namely ξ, η, a, b and G. Since, V(corresponding to $\eta, V = M^{\eta}_{a,b,\xi}$) and G are known only to Alice and Bob, so it is not possible to break this system to anyone. Although the key construction process for a known party is straightforward theoretically, has a large key space and It is highly challenging for an attacker to build a matrix using tuple(ξ, η, a, b). This is the main attraction of our suggested key setup strategies. As the keys η, a, b and ξ are only known to Bob and Alice, the proposed approach ensures the validity and integrity of the data.

References

[1] Asci,, M., Aydinyuz S., k-Order Fibonacci Polynomials on AES-Like Cryptology. *CMES-Computer Modeling in Engineering & Sciences*, 131(1),(2022), 277–293.
[2] DUMMIT, D. S., AND FOOTE, R. M.,*Abstract algebra*, vol. 3. Wiley Hoboken, 2004.
[3] ElGamal, T., A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on information theory* 31, 4 (1985), 469-472.
[4] GOULD, H. W., A history of the Fibonacci q-matrix and a higher-dimensional problem. *Fibonacci Quart* 19, 3 (1981), 250-257.
[5] GUPTA, I., SINGH, J., AND CHAUDHARY, R., Cryptanalysis of an extension of the hill cipher. *Cryptologia* 31, 3 (2007), 246-253.
[6] Kalman, D., AND Mena, R., The Fibonacci Number-Exposed. *The Mathematical Magazine*, 2, (2002).
[7] KOSHY, T., *Fibonacci and Lucas numbers with applications.* John Wiley & Sons, 2019.
[8] KUMARI, M., AND TANTI, J., A model of public key cryptography using multinacci matrices. *arXiv preprint arXiv:2003.08634* (2020).
[9] KUMARI, M., AND TANTI, J., On the role of the Fibonacci matrix as key in modified ecc. *arXiv preprint arXiv:2112.11013* (2021).
[10] MAO, W., *Modern cryptography: theory and practice.* Pearson Education India,2003.
[11] PAAR, C., AND PELZL, J., *Understanding cryptography: a textbook for students and practitioners.* Springer Science & Business Media, 2009.
[12] PRASAD, K., AND MAHATO, H., Cryptography using generalized Fibonacci matrices with an affine-hill cipher. *Journal of Discrete Mathematical Sciences and Cryptography* (2021), 1-12.
[13] PRASAD, K., MAHATO, H. AND KUMARI, M., A novel public key cryptography based on generalized Lucas matrices.*arXiv preprint arXiv:2202.08156v1* (2022).
[14] STALLINGS, W., *Cryptography and network security: principles and practice, 7th Ed.* Pearson Education Limited, 2017.
[15] STINSON, D. R., *Cryptography: theory and practice, 3rd Ed.* Chapman and Hall/CRC, Taylor & Francis Group, 2006.
[16] STOTHERS, A. J., On the complexity of matrix multiplication.
[17] SUNDARAYYA, P. AND VARA PRASAD, G., A public key cryptosystem using affine hill cipher under modulation of prime number. *Journal of Information and Optimization Sciences* 40, 4 (2019), 919-930.
[18] Suleyman Aydinyuz, Mustafa Asci, Error detection and correction for coding theory on k-order Gaussian Fibonacci matrices. *Mathematical Biosciences and Engineering*, 2023, 20(2), 1993-2010. doi: 10.3934/mbe.2023092.

[19] TASCI, D., AND KILIC, E., On the order-k generalized lucas numbers. *Applied mathematics and computation 155*, 3 (2004), 637-641.

[20] THILAKA, B., AND RAJALAKSHMI, K., An extension of hill cipher using generalized inverses and mth residue modulo n. *Cryptologia 29*, 4 (2005), 367-376.

[21] VISWANATH, M., AND KUMAR, M. R., A public key cryptosystem using Hill's cipher. *Journal of Discrete Mathematical Sciences and Cryptography* 18, 1-2 (2015), 129-138.

Vaishali Billore
Institute: Department of Applied Mathematics Institute of Engineering & Technology, Indore (M.P.) 452001, India
Email address: vaishali.billore20@gmail.com

Naresh Patel
Institute: Department of Mathematics, Government Holkar (Model, Autonomous) Science College, Indore (M.P.) 452001, India
Email address: n_patel_1978@yahoo.co.in