Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 3, pp. 809–825
DOI : 10.47974/JDMSC-2045

An approach of encryption that combines ECC and the adjacency matrices of graphs using extended generalized Lucas matrix as key matrix

Vaishali Billore *
Institute of Engineering and Technology
Indore 452001
Madhya Pradesh
India

Naresh Patel †
Government Holkar (Model, Autonomous) Science College
Indore 452001
Madhya Pradesh
India

Hemant Makwana §
Department of Information and Technology
Institute of Engineering and Technology
Indore 452001
Madhya Pradesh
India

Abstract

These days, the best way to secure our data and conversations is to use message encryption techniques. Thanks to the proliferation of network and internet communications, advancements in message encryption technologies have picked up speed. When personal, sensitive information is transmitted via unsecured networks, it opens the door to possible hacking attempts, theft, and eavesdropping on conversations. In order to shorten this term, cryptographic methods are essential. Along with the conventional matrix algebra, we created a higher-order recursive matrix called an Extended generalised Lucas matrix and linked it

* *E-mail:* vaishali.billore20@gmail.com (Corresponding Author)
† *E-mail:* n_patel_1978@yahoo.co.in
§ *E-mail:* hmakwana@ietdavv.edu.in

to Extended generalised Fibonacci sequences in this paper. Elliptic curve cryptography and graph theory are the foundations of our proposed public key cryptography, which employs these matrices as keys for an affine cypher and key agreement for encryption-decryption using a mix of terms from Extended generalised Lucas sequences and residue operations. By reducing key transmission to the exchange of a small set of numbers (parameters) rather than the full key matrix, this method offers a large key space while simultaneously reducing the space and time complexity of key transmission. On top of that, it's secure and dependable since it's built on the challenging Elliptic Curve-Discrete Logarithm algorithm.

Subject Classification (2010): *11B37, 11T71, 11B39, 14H52, 94A60.*

Keywords: *Extended generalized lucas sequence & matrices, Affine hill cipher, Elliptic curve cryptography, Adjacency matrix.*

1. Introduction

Confidentiality in communication has been a top priority for humans ever since the invention of writing, and they have sought out various means to conceal their messages. Due to technical improvements, encryption systems have undergone substantial evolution. Today, the security of encrypted text and information protection in an electronic environment are determined by the cryptography or coding-decoding process and the secrecy of the key. Many of matrix theory's peculiarities depend on the matrix's construction, the interactions of its eigenvalues, and the design of its invertibility structure, among other things. Multiple branches of science make use of engineering and technology based on matrix principles. It is fascinating to see Fibonacci and Lucas sequences applied. Mathematical concepts like the Fibonacci and Lucas series are often used. Some examples of these areas of study are calculus, group theory, linear algebra, and applied mathematics [10]. Furthermore, these figures have several important applications in many fields, such as statistics, biology, computer science, and physics. By employing matrices and generalizing the idea, Ozkan E. and Altun I. [13] could derive the terms of n-step Lucas polynomials. They subsequently established the connection between Lucas polynomials and Fibonacci polynomials. With the help of two digital signatures, Viswanath and Kumar [23], created a public key cryptosystem that uses Hill's cipher and is secure. Public key cryptography utilizing generalized Fibonacci matrices have been introduced by Prasad K. and Mahato H. [15], in which submit numbers rather than matrices. As a result, it improves cryptography technique and minimize complexity. In [16], Prasad K. et al. have introduced novel public key cryptography based on generalized lucas matrices. See [3, 19, 20, 22] for some recent research on studying cryptography using number sequences, related matrices, and traditional cryptography. Graph theory ideas are an important resource for cryptography and have numerous uses in mathematics. Cryptography uses graph theory in many different ways [5]. In [25], the lower triangular matrix utilized as the key matrix in an encryption scheme that used a

full graph and its Hamiltonian Walk. In [1] they described a unique approach to message encoding and decoding using graph labelling. In both cases, an upper triangular matrix was employed as a key matrix. [24, 25] explained the symmetric encryption technique utilizing a cycle graph, complete graph, and minimal spanning tree. In [12], Mohan P. et al. described a self-invertible key matrix encryption method based on the adjacency matrices of specific graphs. Singh et.al. [18] reviewed ECC over RSA, see also [9, 14, 21]. A unique technique to the ECC that uses matrices with ElGamal algorithm was presented by Balamurugan et al. [2]. Singh and Debbarma [17] have proposed a solution to the problem of large key size that requires high computational power devices. Based on the matrix approach, Geetha and Jain [8] offered a fast-mapping method for ECC that delivers excellent security for an encrypted message. In [4], V. Billore, N. Patel and H. Makwana introduced Extended Generalized Fibonacci Matrix as key matrix for modified ECC.

By using the trace of the associated Extended Generalised Fibonacci matrices, we can derive the terms of an Extended Generalised Lucas sequence, which in turn extends the generalised Lucas sequence to higher orders while preserving its Fibonacci trace properties, which is the main focus of this research. In order to establish a relationship between them, recursive matrices have been generated using extended generalised Fibonacci matrices (EGFM) [3]. Additionally, we apply these matrices to the Affine-Hill method with adjacency matrix using Elliptic curve cryptography and assess its performance.

2. Preliminaries

2.1 *Graph*

A graph is an ordered pair consisting of a set of vertices and edges.

2.2 *Adjacency Matrix*

An adjacency matrix is a square matrix that represents a finite graph. The elements of matrix denote whether two vertices in a graph are adjacent or not.

2.3 *Elliptic curve Definition* [6, 11]

An elliptic curve E is constructed over $\mathbb{F}_p$ by the set of points (y, z) with $y, z \in \mathbb{F}_p$ that satisfy the equation

$$z^2 = y^3 + my + n \qquad (2.1)$$

with $m, n \in \mathbb{F}_p$, such that $4m^3 + 27n \neq 0 \ (mod\ p)$ and by a single element denoted by $\mathcal{O}$, known as the point at infinity. The elliptic curve over $\mathbb{F}_p$ is expressed by $E_{\mathbb{F}_p}(m, n)$. The points on $E_{\mathbb{F}_p}(m, n)$ form an additive abelian group, with $\mathcal{O}$ as its identity element.

2.4 *Public Key Setup and Key exchanging*

For public key setup & key exchanging, we use the Elgamal technique [7]. For that first choice, a prime number p and primitive root of p say γ. Also, select a private key z i.e. $1 < z < \varphi(p)$. Then construct $\mu_1 = \gamma$ and $\mu_2 =$

$\gamma^z \ (mod\ p)$. As a result, (p, μ_1, μ_2) will be created as the public key and z will be retained as the private key. Assume for a moment that the Sender and Receiver wish to interact with one another. Next, Sender first chooses a random integer ϵ i.e. $1 < \epsilon < \varphi(p)$. Further, using a public key (p, μ_1, μ_2) construct signature key (say i) such that $i = \mu_1^{\epsilon}\ (mod\ p)$ and secret key $h = \mu_2^{\epsilon}\ (mod\ p)$ for encryption. Now, Sender can encrypt the plaintext using the above signature key & secret key and send (i, c) to Receiver. Where c is the corresponding ciphertext.

2.5 *Key recovery by Receiver*

After getting (i, c) from Sender, Receiver recover h using their secret key z as:

$$h = i^z\ (mod\ p) \equiv (\mu_1^{\epsilon})^z\ (mod\ p) \equiv (\mu_1^z)^{\epsilon}\ (mod\ p) \equiv \mu_2^{\epsilon}\ 2\ (mod\ p).$$

Using this secret key h, Receiver will recovers the plaintext Successfully.

2.6 *Extended Generalized Fibonacci Sequences and Matrix Construction*

For $\theta \in \mathbb{Z}$, the ζ^{th} order Extended generalized Fibonacci sequence is defined with the following recurrence relation:

$$g_{\alpha,\beta,\zeta+\theta} = \alpha^{\zeta-1} g_{\alpha,\beta,\zeta+\theta-1} + \alpha^{\zeta-2}\beta g_{\alpha,\beta,\zeta+\theta-2} + \ldots + \alpha\beta^{\zeta-2} g_{\alpha,\beta,\theta+1} + \beta^{\zeta-1} g_{\alpha,\beta,\theta}\ ,\ \zeta(\geq 2), \alpha, \beta \in N \quad (2.2)$$

with initial values $g_{\alpha,\beta,0} = g_{\alpha,\beta,1} = \ldots = g_{\alpha,\beta,\zeta-2} = 0,\ g_{\alpha,\beta,\zeta-1} = 1.$

The corresponding Extended generalized Fibonacci matrix $M_{\alpha,\beta,\zeta}^{\theta}$ of order ζ is defined [3,4] as

$$M_{\alpha,\beta,\zeta}^{\theta} = \begin{pmatrix} g_{\alpha,\beta,\zeta+\theta-1} & \alpha^{\zeta-2}\beta g_{\alpha,\beta,\zeta+\theta-2} + \alpha^{\zeta-3}\beta^2 g_{\alpha,\beta,\zeta+\theta-3} + \cdots + \beta^{\zeta-1} g_{\alpha,\beta,\theta} \\ g_{\alpha,\beta,\zeta+\theta-2} & \alpha^{\zeta-2}\beta g_{\alpha,\beta,\zeta+\theta-3} + \alpha^{\zeta-3}\beta^2 g_{\alpha,\beta,\zeta+\theta-4} + \cdots + \beta^{\zeta-1} g_{\alpha,\beta,\theta-1} \\ \vdots & \vdots \\ g_{\alpha,\beta,\theta+1} & \alpha^{\zeta-2}\beta g_{\alpha,\beta,\theta} + \alpha^{\zeta-3}\beta^2 g_{\alpha,\beta,\theta-1} + \cdots + \beta^{\zeta-1} g_{\alpha,\beta,-\zeta+\theta+2} \\ g_{\alpha,\beta,\theta} & \alpha^{\zeta-2}\beta g_{\alpha,\beta,\theta-1} + \alpha^{\zeta-3}\beta^2 g_{\alpha,\beta,\theta-2} + \cdots + \beta^{\zeta-1} g_{\alpha,\beta,-\zeta+\theta+1} \end{pmatrix}$$

$$\begin{pmatrix} \alpha^{\zeta-3}\beta^2 g_{\alpha,\beta,\zeta+\theta-2} + \alpha^{\zeta-4}\beta^3 g_{\alpha,\beta,\zeta+\theta-3} + \cdots + \beta^{\zeta-1} g_{\alpha,\beta,\theta+1} & \cdots & \beta^{\zeta-1} g_{\alpha,\beta,\zeta+\theta-2} \\ \alpha^{\zeta-3}\beta^2 g_{\alpha,\beta,\zeta+\theta-3} + \alpha^{\zeta-4}\beta^3 g_{\alpha,\beta,\zeta+\theta-4} + \cdots + \beta^{\zeta-1} g_{\alpha,\beta,\theta} & \cdots & \beta^{\zeta-1} g_{\alpha,\beta,\zeta+\theta-3} \\ \vdots & \ddots & \vdots \\ \alpha^{\zeta-3}\beta^2 g_{\alpha,\beta,\theta} + \alpha^{\zeta-4}\beta^3 g_{\alpha,\beta,\theta-1} + \cdots + \beta^{\zeta-1} g_{\alpha,\beta,-\zeta+\theta+3} & \cdots & \beta^{\zeta-1} g_{\alpha,\beta,\theta} \\ \alpha^{\zeta-3}\beta^2 g_{\alpha,\beta,\theta-1} + \alpha^{\zeta-4}\beta^3 g_{\alpha,\beta,\theta-2} + \cdots + \beta^{\zeta-1} g_{\alpha,\beta,-\zeta+\theta+2} & \cdots & \beta^{\zeta-1} g_{\alpha,\beta,\theta-1} \end{pmatrix} \quad (2.3)$$

where the starting matrices are provided by

$$M^{1}_{\alpha,\beta,\zeta} = \begin{pmatrix} \alpha^{\zeta-1} & \alpha^{\zeta-2}\beta & \dots & \alpha\beta^{\zeta-2} & \beta^{\zeta-1} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}_{\zeta\times\zeta} \quad \text{and}$$

$$M^{-1}_{\alpha,\beta,\zeta} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ \frac{1}{\beta^{\zeta-1}} & \frac{-\alpha^{\zeta-1}}{\beta^{\zeta-1}} & \frac{-\alpha^{\zeta-2}}{\beta^{\zeta-2}} & \dots & \frac{-\alpha}{\beta} \end{pmatrix}_{\zeta\times\zeta}$$

Theorem 2.1: *If* $(\zeta \geq 2), \alpha, \beta \in \mathbb{N}, \theta \in \mathbb{Z}, M^{\theta}_{\alpha,\beta,\zeta}$ *be Extended generalized Fibonacci matrices (EGFM) and* I_{ζ} *is a Unit matrix of order* ζ *then for all* ζ *and* θ *following conditions hold*

(i) $(M^{1}_{\alpha,,\beta,\zeta}\ )\,\theta = M^{\theta}_{\alpha,,\beta,\zeta}$ and $\left(M^{-1}_{\alpha,\beta,\zeta}\ \right)\theta = M^{-\theta}_{\alpha,\beta,\zeta}$.

(ii) $M^{\theta}_{\alpha,,\beta,\zeta}\, M^{-\theta}_{\alpha,\beta,\zeta} = M^{0}_{\alpha,\beta,\zeta} = I_{\zeta}$.

(iii) $det(M^{\theta}_{\alpha,\beta,\zeta}\ ) = [(-\beta)^{\zeta-1}]^{\theta} = (-\beta)^{\theta(\zeta-1)}$.

3. Extended Generalized Lucas Matrices (EGLM)

Now, we are creating a new sequence called $N_{\zeta,\theta}$ that is equivalent to an Extended generalized Fibonacci sequence as seen below.

Definition 1: For $\theta \geq 0$ and $\zeta(\geq 2), \alpha, \beta \in \mathbb{N}$, Consider a recurrence relation of order (ζ) defined as

$$N_{\alpha,\beta,\zeta+\theta} = \alpha^{\zeta-1} N_{\alpha,\beta,\zeta+\theta-1} + \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta+\theta-2} + \dots + \alpha\beta^{\zeta-2} N_{\alpha,\beta,\theta+1} + \beta^{\zeta-1} N_{\alpha,\beta,\theta}$$

with $N_{\alpha,\beta,r} = trace(M^{r}_{\alpha,,\beta,\zeta}\ ), 0 \leq r < \zeta$.

We look at the trace of the first ζ order extended generalized Fibonacci matrices to obtain the starting values for the aforementioned proposed sequences. Since an Extended Generalized Fibonacci Sequence is two ended sequence, Consequently, it is possible to extend the preceding sequence in the reverse direction. We refer to the new sequence mentioned above as the Extended Generalized Lucas Sequence. Here, the recursive matrix of order ζ and for $\theta \in \mathbb{Z}$ related to the aforementioned proposed sequence can be expressed as

$$N^{\theta}_{\alpha,\beta,\zeta} = \begin{pmatrix} N_{\alpha,\beta,\zeta+\theta-1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta+\theta-2} + \alpha^{\zeta-3}\beta^{2} N_{\alpha,\beta,\zeta+\theta-3} + \dots + \beta^{\zeta-1} N_{\alpha,\beta,\theta} \\ N_{\alpha,\beta,\zeta+\theta-2} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta+\theta-3} + \alpha^{\zeta-3}\beta^{2} N_{\alpha,\beta,\zeta+\theta-4} + \dots + \beta^{\zeta-1} N_{\alpha,\beta,\theta-1} \\ \vdots & \vdots \\ N_{\alpha,\beta,\theta+1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\theta} + \alpha^{\zeta-3}\beta^{2} N_{\alpha,\beta,\theta-1} + \dots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+\theta+2} \\ N_{\alpha,\beta,\theta} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\theta-1} + \alpha^{\zeta-3}\beta^{2} N_{\alpha,\beta,\theta-2} + \dots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+\theta+1} \end{pmatrix}$$

$$\begin{pmatrix} \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+\theta-2} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta+\theta-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,\theta+1} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta+\theta-2} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+\theta-3} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta+\theta-4} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,\theta} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta+\theta-3} \\ \vdots & \ddots & \vdots \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\theta} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\theta-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+\theta+3} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\theta} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\theta-1} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\theta-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+\theta+2} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\theta-1} \end{pmatrix} \tag{3.1}$$

and the Extended Generalized Lucas matrix of order ζ is represented by the matrix $N^{\theta}_{\alpha,\beta,\zeta}$, which we indicated by EGLM(ζ,θ). Additionally, the initially created $N^{(0)}_{\alpha,\beta,\zeta}$ Extended Generalized Lucas matrix is

$$N^{(0)}_{\alpha,\beta,\zeta} = \begin{pmatrix} N_{\alpha,\beta,\zeta-1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta-2} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,0} \\ N_{\alpha,\beta,\zeta-2} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta-3} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-4} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-1} \\ \vdots & \vdots \\ N_{\alpha,\beta,1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,0} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+2} \\ N_{\alpha,\beta,0} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,-1} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+1} \end{pmatrix}$$

$$\begin{pmatrix} \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-2} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,1} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta-2} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-3} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta-4} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,0} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta-3} \\ \vdots & \ddots & \vdots \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,0} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+3} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,0} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,-1} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+2} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,-1} \end{pmatrix} \tag{3.2}$$

Example 1: Of order two and three, Initial Extended Generalized Lucas matrices are respectively

$$\begin{pmatrix} \alpha^2 & \beta \\ 2 & -\alpha \end{pmatrix}, \qquad \begin{pmatrix} \alpha^4 + 2\alpha\beta & \alpha^3\beta + 3\beta^2 & \alpha^2\beta^2 \\ \alpha^2 & 2\alpha\beta & 3\beta^2 \\ 3 & -2\alpha^2 & -\alpha\beta \end{pmatrix}$$

Theorem 3.1: *If $\theta \in \mathbb{Z}, M^{\theta}_{\alpha,\beta,\zeta}$ represents an Extended Generalized Fibonacci matrix and $N^{\theta}_{\alpha,\beta,\zeta}$ be EGLM(ζ,θ). Assuming $N^{(0)}_{\alpha,\beta,\zeta}$ is initial matrix as specified by equation (3.2), then we obtain*

$$N^{\theta}_{\alpha,\beta,\zeta} = M^{\theta}_{\alpha,\beta,\zeta} N^{(0)}_{\alpha,\beta,\zeta} = N^{(0)}_{\alpha,\beta,\zeta} M^{\theta}_{\alpha,\beta,\zeta}$$

Proof: For $\theta \geq 1$, we use mathematical induction to demonstrate it. Clearly the result is true for $\theta = 0$. We have when $\theta = 1$

$$N^{(0)}_{\alpha,\beta,\zeta} M^{1}_{\alpha,\beta,\zeta} = \begin{pmatrix} N_{\alpha,\beta,\zeta-1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta-2} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,0} \\ N_{\alpha,\beta,\zeta-2} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta-3} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-4} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-1} \\ \vdots & \vdots \\ N_{\alpha,\beta,1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,0} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+2} \\ N_{\alpha,\beta,0} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,-1} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+1} \end{pmatrix}$$

$$\begin{pmatrix} \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-2} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,1} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta-2} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-3} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta-4} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,0} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta-3} \\ \vdots & \ddots & \vdots \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,0} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+3} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,0} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,-1} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+2} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,-1} \end{pmatrix}$$

$$\times \begin{pmatrix} \alpha^{\zeta-1} & \alpha^{\zeta-2}\beta & \ldots & \alpha\beta^{\zeta-2} & \beta^{\zeta-1} \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

Using the recurrence relation $N_{\zeta,\theta}$ and equation (3.1), we get

$$= \begin{pmatrix} N_{\alpha,\beta,\zeta} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta-1} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,1} \\ N_{\alpha,\beta,\zeta-1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta-2} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,0} \\ \vdots & \vdots \\ N_{\alpha,\beta,2} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,1} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,0} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+3} \\ N_{\alpha,\beta,1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,0} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+2} \end{pmatrix}$$

$$\begin{pmatrix} \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-1} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,2} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta-1} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta-2} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,1} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta-2} \\ \vdots & \ddots & \vdots \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,1} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,0} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+2} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,1} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,0} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+3} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,0} \end{pmatrix} = N^1_{\alpha,\beta,\zeta}$$

Now, assuming that the result is true for $\theta = k$ i.e. $N^{(0)}_{\alpha,\beta,\zeta} M^k_{\alpha,\beta,\zeta} = N^k_{\alpha,\beta,\zeta}$. Further, we show that the statement is also true for $\theta = k + 1$. we have,

$$N^{(0)}_{\alpha,\beta,\zeta} M^{k+1}_{\alpha,\beta,\zeta} = N^{(0)}_{\alpha,\beta,\zeta} M^k_{\alpha,\beta,\zeta} M^1_{\alpha,\beta,\zeta} = N^k_{\alpha,\beta,\zeta} M^1_{\alpha,\beta,\zeta}$$

$$= \begin{pmatrix} N_{\alpha,\beta,\zeta+k-1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta+k-2} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+k-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,k} \\ N_{\alpha,\beta,\zeta+k-2} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta+k-3} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+k-4} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,k-1} \\ \vdots & \vdots \\ N_{\alpha,\beta,k+1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,k} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,k-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+k+2} \\ N_{\alpha,\beta,k} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,k-1} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,k-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+k+1} \end{pmatrix}$$

$$\begin{pmatrix} \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+k-2} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta+k-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,k+1} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta+k-2} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+k-3} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta+k-4} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,k} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta+k-3} \\ \vdots & \ddots & \vdots \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,k} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,k-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+k+3} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,k} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,k-1} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,k-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+k+2} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,k-1} \end{pmatrix}$$

$$\times M^1_{\alpha,\beta,\zeta}$$

Using the recurrence relation $N_{\zeta,\theta}$ and equation (3.1), we get

$$= \begin{pmatrix} N_{\alpha,\beta,\zeta+k} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta+k-1} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+k-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,k+1} \\ N_{\alpha,\beta,\zeta+k-1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,\zeta+k-2} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+k-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,k} \\ \vdots & \vdots \\ N_{\alpha,\beta,k+2} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,k+1} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,k} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+k+3} \\ N_{\alpha,\beta,k+1} & \alpha^{\zeta-2}\beta N_{\alpha,\beta,k} + \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,k-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+k+2} \end{pmatrix}$$

$$\begin{pmatrix} \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+k-1} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta+k-2} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,k+2} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta+k-1} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,\zeta+k-2} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,\zeta+k-3} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,k+1} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,\zeta+k-2} \\ \vdots & \ddots & \vdots \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,k+1} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,k} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+k+2} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,k1} \\ \alpha^{\zeta-3}\beta^2 N_{\alpha,\beta,k} + \alpha^{\zeta-4}\beta^3 N_{\alpha,\beta,k-1} + \cdots + \beta^{\zeta-1} N_{\alpha,\beta,-\zeta+k+1} & \cdots & \beta^{\zeta-1} N_{\alpha,\beta,k} \end{pmatrix}$$

$$= N^{k+1}_{\alpha,\beta,\zeta}.$$

Consider the negative direction as $\theta = -k$, where $k \geq 0$. Then, using a similar reasoning, it may be demonstrated for negative direction by mathematical induction on k. When combining both situations, the conclusion is true for every $\theta \in \mathbb{Z}$. Similar to the first equality, the second equality can be proven.

Theorem 3.2: *An Extended generalised Lucas matrices determinant is provided by*

$$\det(\mathrm{N}^{\theta}_{\alpha,\beta,\zeta}) = \begin{cases} \beta^{(\zeta-1)\theta}\det\left(\mathrm{N}^{0}_{\alpha,\beta,\zeta}\right) & \text{if } \zeta = \text{odd} \\ (-1)^{\theta}\beta^{(\zeta-1)\theta}\det(\mathrm{N}^{0}_{\alpha,\beta,\zeta}) & \text{if } \zeta = \text{even} \end{cases}$$

Proof:

$$det(N^{\theta}_{\alpha,\beta,\zeta}) = det(M^{\theta}_{\alpha,\beta,\zeta}\, N^{0}_{\alpha,\beta,\zeta}) = det(M^{\theta}_{\alpha,\beta,\zeta}) det(N^{0}_{\alpha,\beta,\zeta})$$

$$= (-\beta)^{(\zeta-1)\theta}\det\left(N^{0}_{\alpha,\beta,\zeta}\right)$$

$$= \begin{cases} \beta^{(\zeta-1)\theta}\det\left(\mathrm{N}^{0}_{\alpha,\beta,\zeta}\right) & \text{if } \zeta = \text{odd} \\ (-1)^{\theta}\beta^{(\zeta-1)\theta}\det\left(\mathrm{N}^{0}_{\alpha,\beta,\zeta}\right) & \text{if } \zeta = \text{even} \end{cases}.$$

Theorem 3.3: *If $M^{\theta}_{\alpha,\beta,\zeta}$ is the EGFM(ζ,θ) and $N^{\theta}_{\alpha,\beta,\zeta}$ is the ζ^{th} order Extended generalised Lucas matrix, then $N^{\theta}_{\alpha,\beta,\zeta}\, N^{-\theta}_{\alpha,\beta,\zeta} = R\ \forall\ \theta \in \mathbb{Z}$, where $R = \left(N^{0}_{\alpha,\beta,\zeta}\right)^2$.*

Proof: $\forall\ \theta \in \mathbb{Z}$, we have

$$N^{\theta}_{\alpha,\beta,\zeta}\, N^{-\theta}_{\alpha,\beta,\zeta} = M^{\theta}_{\alpha,\beta,\zeta}\, N^{0}_{\alpha,\beta,\zeta}\, M^{-\theta}_{\alpha,\beta,\zeta}\, N^{0}_{\alpha,\beta,\zeta} = M^{\theta}_{\alpha,\beta,\zeta} M^{-\theta}_{\alpha,\beta,\zeta}\, N^{0}_{\alpha,\beta,\zeta}\, N^{0}_{\alpha,\beta,\zeta} = I_{\zeta} R = R.$$

Theorem 3.4: *If $R = \left(N^{0}_{\alpha,\beta,\zeta}\right)^2$ is invertible and $N^{\theta}_{\alpha,\beta,\zeta}$ is a EGLM(ζ,θ), then the inverse is provided by $Inv(N^{\theta}_{\alpha,\beta,\zeta}) = N^{-\theta}_{\alpha,\beta,\zeta}\, R^{-1}$.*

Proof: Since we have $N^{\theta}_{\alpha,\beta,\zeta}\, N^{-\theta}_{\alpha,\beta,\zeta} = R$ and $N^{0}_{\alpha,\beta,\zeta}$ is an invertible matrix, R follows. Now, after post-multiplying with R^{-1}, we obtain $N^{\theta}_{\alpha,\beta,\zeta}\ (N^{-\theta}_{\alpha,\beta,\zeta} R^{-1}) =$

I_ζ , where I_ζ is the identity matrix. As a result, for each EGLM $N^{\theta}_{\alpha,\beta,\zeta}$, there is a special matrix ($N^{-\theta}_{\alpha,\beta,\zeta}R^{-1}$) whose product with $N^{\theta}_{\alpha,\beta,\zeta}$ is an identity matrix. Hence

$$Inv\left(N^{\theta}_{\alpha,\beta,\zeta}\right) = N^{-\theta}_{\alpha,\beta,\zeta}\,R^{-1}.$$

Theorem 3.5: *Let for any matrix* $M = (m_{ij})$, *we obtain*

$$M\ (mod\ p) = [m_{ij}\ (mod\ p)].$$

4. Scheme and Algorithm for Encryption

This section provided a detailed description of the proposed approach, involving the extended generalized Lucas matrix as the key matrix in along with elliptic curve cryptography, the Elgamal technique, and the graph adjacency matrices. Assume we have a public key pk(p, μ_1, μ_2), where μ_1 and μ_2 are parts of the public key that Receiver (the recipient) generated by private key z. Now, the secret key can be determined by using this public key (See in section 2). Key matrix U will be provided after secret key has been generated.

Algorithm for encryption (sender having knowledge of pk$(\boldsymbol{p}, \mu_1, \mu_2)$):

1. First, note that the message unit's initial letter is the distinctive character A. The necessary graph is created by joining the consecutive letters in the provided plain text message units.
2. Using $E_{\mathbb{F}_p}(m, n)$, the message components have been transformed into corresponding

numerical values.

3. The computation of edge weights in the graph involves determining the numerical difference among two adjacent vertices.
4. addition modulo p was taken to create the adjacency matrix P of plain text for the graph.
5. Sender chooses secret number ϵ, such as $1 < \epsilon < \varphi(p)$.
6. The Signature is $\nu \leftarrow \mu_1^{\epsilon}\ (mod\ p)$.
7. The Secret key is $\psi \leftarrow \mu_2^{\epsilon}\ (mod\ p)$.
8. Initiate Extended generalized Lucas sequence $N_{\alpha,\beta,\psi,\nu}$ of order ψ, with considering value of α, β.
9. **Key matrix:** $U \leftarrow N^{(\nu)}_{\alpha,\beta,\psi}$, where $\{N_{\alpha,\beta,\psi}\}$ is Extended generalized Lucas matrix by choosing the value of α, β of order $\psi \times \psi$.
10. **Encryption:** $\rho \equiv Enc(e_m) : \rho \leftarrow (P_{\psi\times\psi}U_{\psi\times\psi} + \psi XL_{\psi\times\psi})\ (mod\ p)$ where

$$L = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{bmatrix}_{\psi \times \psi}$$

11. transmit (ρ, ν, α, β)

Decryption Algorithm: After receiving $(\rho, \nu, \alpha, \beta)$

1. The Secret key is $\psi \leftarrow \nu^z \ (mod\ p)$, with z as Receiver Secret key.
2. Initiate Extended generalized Lucas sequence $\{N_{\alpha,\beta,\psi,\nu}\}$ using values of α, β
3. **Key Matrix:** $U^* \leftarrow N_{\alpha,\beta,\psi}^{(-\nu)} R^{-1}$, where both $N_{\alpha,\beta,\psi}^{(-\nu)}$ & $R = \left(N_{\alpha,\beta,\psi}^{0}\right)^2$ may be obtained from step 2 using (3.1), (3.2).
4. **Decryption:** $P \equiv Dec(\rho) \leftarrow \left(\rho_{\psi\times\psi} - \psi XL\right) U^*_{\psi\times\psi} \ \ (mod\ p)$ where
$$L = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{bmatrix}_{\psi \times \psi}.$$
5. Lastly, for final matrix $P_{\psi\times\psi}$ of previous step using addition modulo p, the receiver will get the adjacency matrix for plain text of the needed graph.
6. The receiver will generate the required graph using nodes and a few specified weights after reconstructing the graph.
7. To compute the message, the weights are added to their related vertices. We know that vertex v_1 is denoted by letter A with corresponding value, that v_2 is equal to v_1 plus the weight e_1, and so on.
8. Plaintext (P) recovered.

Example 2: Using the suggested scheme mentioned above, Encrypt the plaintext SUN. Solution. Consider the elliptic curve $z^2 = y^3 + 33y + 43\ (mod\ p)$ and denoted by $E_{\mathbb{F}_{47}}(33, 43)$. Also, we have $|E_{\mathbb{F}_{47}}(33, 43)| = 47$.

The points of $E_{\mathbb{F}_{47}}(33, 43)$ are:

(3,13)	(3,34)	(4,2)	(4,45)	(5,2)	(5,45)	(6,9)	(6,38)	(7,10)	(7,37)
(13,15)	(13,32)	(14,10)	(14,37)	(15,23)	(15,24)	(16,22)	(16,25)	(17,21)	(17,26)
(19,3)	(19,44)	(20,14)	(20,33)	(24,18)	(24,29)	(26,10)	(26,37)	(29,3)	(29,44)
(30,16)	(30,31)	(31,5)	(31,42)	(32,11)	(32,36)	(34,7)	(34,40)	(35,9)	(35,38)
(38,2)	(38,45)	(45,4)	(45,43)	(46,3)	(46,44)	$\mathcal{O}$			

Assume that the generator point of $E_{\mathbb{F}_{47}}(33, 43)$ is $X = (4, 2)$. Now the letters, symbols, numbers and special characters are mapped as following:

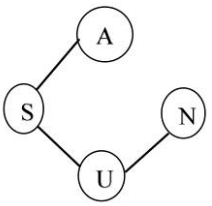
A	B	C	D	E	F	G	H	I	J
(4,2)	(29,44)	(46,44)	(45,4)	(19,3)	(38,2)	(5,45)	(7,10)	(17,26)	(13,32)
K	L	M	N	O	P	Q	R	S	T
(15,24)	(32,36)	(6,9)	(14,10)	(24,29)	(20,14)	(3,34)	(30,31)	(31,42)	(16,22)

U (35,9)	V (26,37)	W (34,40)	X (34,7)	Y (26,10)	Z (35,38)	0 (16,25)	1 (31,5)	2 (30,16)	3 (3,13)
4 (20,33)	5 (24,18)	6 (14,37)	7 (6,38)	8 (32,11)	9 (15,23)	~ (13,15)	Blank/space(■) (17,21)	@ (7,37)	% (5,2)
& (38,45)	$ (19,44)	- (45,43)	/ (46,3)	. (29,3)	# (4,45)	* $\mathcal{O}$			

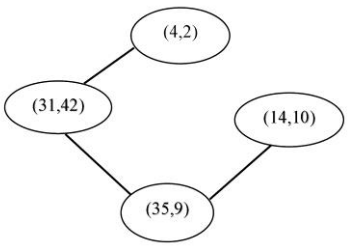
(Construction of Public Key:) Assume that $p = 47$, primitive root says $\gamma = 43$ and private key $z = 24$ selected by Receiver. Then, $\mu_1 = \gamma$ and $\mu_2 = (43)^{24} \ (mod\ 47) \equiv 4$. Thus, Receiver public key is $(47, 43, 4)$.

Key Generation and Encryption

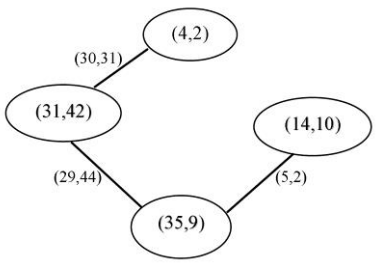
The supplied plaintext message units should first have the special character A added as the first letter. Next, the message A SUN, should be converted to the graph's vertices. Connecting the vertices from vertex 1 to 4 are the defined message units sequential letters.



We obtain via an encoded table, $A \rightarrow (4, 2), S \rightarrow (31, 42), U \rightarrow (35, 9)$ and $N \rightarrow (14, 10)$.



Finding the numerical separation between the following two connected vertices and taking the addition modulo 47 yields the weights of the graph's edges.



The adjacency matrix that corresponds to the above graph has been calculated and assigned the letter P.

$$P = \begin{pmatrix} 0 & (30,31) & 0 & 0 \\ (30,31) & 0 & (29,44) & 0 \\ 0 & (29,44) & 0 & (5,2) \\ 0 & 0 & (5,2) & 0 \end{pmatrix}$$

Using above public key Sender can create an encryption key and encrypt message as follow: First choose $1 < \epsilon < \varphi(p),\ let\ \epsilon = 24$.

Calculating signature $\nu = \mu_1^{\epsilon} = (43)^{24}\ (mod\ q) \equiv 4$ and secret key $\psi = \mu_2^{\epsilon} = (4)^{24}\ (mod\ q) \equiv 4$ and the key matrix $U = N_{\alpha,\beta,\psi}^{(\nu)}\ (mod\ q)$ for encryption is given by

$U = N_{2,3,4}^{(4)}$

$$= \begin{pmatrix} N_{2,3,7} & 12N_{2,3,6} + 18N_{2,3,5} + 27N_{2,3,4} & 18N_{2,3,6} + 27N_{2,3,5} & 27N_{2,3,6} \\ N_{2,3,6} & 12N_{2,3,5} + 18N_{2,3,4} + 27N_{2,3,3} & 18N_{2,3,5} + 27N_{2,3,4} & 27N_{2,3,5} \\ N_{2,3,5} & 12N_{2,3,4} + 18N_{2,3,3} + 27N_{2,3,2} & 18N_{2,3,4} + 27N_{2,3,3} & 27N_{2,3,4} \\ N_{2,3,4} & 12N_{2,3,3} + 18N_{2,3,2} + 27N_{2,3,1} & 18N_{2,3,3} + 27N_{2,3,2} & 27N_{2,3,3} \end{pmatrix} (mod\ 47)$$

$$i.e.\ U \equiv \begin{pmatrix} 31 & 28 & 30 & 6 \\ 42 & 24 & 41 & 26 \\ 41 & 43 & 2 & 8 \\ 9 & 16 & 29 & 28 \end{pmatrix} \quad (mod\ 47).$$

Encryption: $\rho \leftarrow (P_{\psi\times\psi} U_{\psi\times\psi} + \psi X L_{\psi\times\psi})\ (mod\ 47)$.

$$\rho = (P\ U + \psi x L)$$

$$\equiv \left[\begin{pmatrix} 0 & (30,31) & 0 & 0 \\ (30,31) & 0 & (29,44) & 0 \\ 0 & (29,44) & 0 & (5,2) \\ 0 & 0 & (5,2) & 0 \end{pmatrix} \begin{pmatrix} 31 & 28 & 30 & 6 \\ 42 & 24 & 41 & 26 \\ 41 & 43 & 2 & 8 \\ 9 & 16 & 29 & 28 \end{pmatrix} + (45,4) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \right] \quad (mod\ 47)$$

$$\equiv \begin{bmatrix} (7,10) & (6,9) & (13,15) & (29,44) \\ (14,37) & (3,13) & (20,33) & (6,38) \\ (26,10) & (6,38) & (34,7) & (4,2) \\ (4,45) & (24,18) & (13,15) & (19,44) \end{bmatrix} \equiv \begin{bmatrix} H & M & \sim & B \\ 6 & 3 & 4 & 7 \\ Y & 7 & X & A \\ \# & 5 & \sim & \$ \end{bmatrix}$$

Thus, sender encrypted the plaintext **A SUN** to **HM~B6347#5~$**. and send it to receiver along with his signature i.e. $\{\nu = 3, \alpha = 2, \beta = 3, \rho = HM{\sim}B6347\#5{\sim}\$\}$.

Decryption: After receiving $(\nu, \alpha, \beta, \rho)$ from sender. To construct decryption key U^* first recover ψ using their secret key z as follows:

$$\psi = v^z \,(mod\ 47) = 4^{24}\,(mod\ 47) \equiv 4.$$

$$Thus,\ U^* = N_{\alpha,\beta,\psi}^{(-v)}\, R^{-1}\,(mod\ 47)\ where\ R = \left(N_{\alpha,\beta,\psi}^{(0)}\right)^2$$

$$i.e.\ U^* = N_{2,3,4}^{(-3)}\, R^{-1}\,(mod\ 47)\ where\ R = \left(N_{2,3,4}^{(0)}\right)^2$$

$$U^* = \begin{bmatrix} 14 & 32 & 21 & 15 \\ 11 & 20 & 41 & 11 \\ 30 & 6 & 36 & 18 \\ 32 & 9 & 45 & 24 \end{bmatrix} \quad (mod\ 47)$$

Clearly $UU^* = I\ (mod\ 47)$.

Thus, plaintext obtained by $P \leftarrow \left(\rho_{\psi\times\psi} - \psi X L_{\psi\times\psi}\right) U^*_{\psi\times\psi}\ (mod\ 47)$

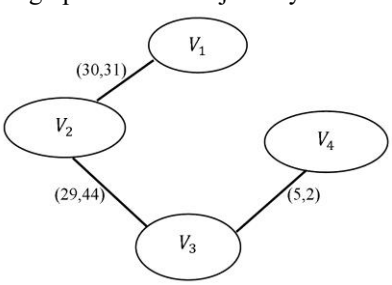
$P = (\rho - \psi x L).U^*$

$$\equiv \left(\begin{bmatrix} (7,10) & (6,9) & (13,15) & (29,44) \\ (14,37) & (3,13) & (20,33) & (6,38) \\ (26,10) & (6,38) & (34,7) & (4,2) \\ (4,45) & (24,18) & (13,15) & (19,44) \end{bmatrix} - (45,4) \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \right) \begin{bmatrix} 14 & 32 & 21 & 15 \\ 11 & 20 & 41 & 11 \\ 30 & 6 & 36 & 18 \\ 32 & 9 & 45 & 24 \end{bmatrix} (mod\ 47)$$

$$\equiv \left(\begin{bmatrix} (7,10) & (6,9) & (13,15) & (29,44) \\ (14,37) & (3,13) & (20,33) & (6,38) \\ (26,10) & (6,38) & (34,7) & (4,2) \\ (4,45) & (24,18) & (13,15) & (19,44) \end{bmatrix} + (45,43) \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \right) \begin{bmatrix} 14 & 32 & 21 & 15 \\ 11 & 20 & 41 & 11 \\ 30 & 6 & 36 & 18 \\ 32 & 9 & 45 & 24 \end{bmatrix} (mod\ 47)$$

$$\equiv \begin{bmatrix} 0 & (30,31) & 0 & 0 \\ (30,31) & 0 & (29,44) & 0 \\ 0 & (29,44) & 0 & (5,2) \\ 0 & 0 & (5,2) & 0 \end{bmatrix}$$

Next, construct the graph of above adjacency matrix.



The numerical equivalent value of each vertex was added to the corresponding edge to create the vertices or nodes, of the above graph. The special character A at the beginning tells us that the first vertex must be (4, 2), so finding the other vertices involves letting $V_1 = (4,2)$. As a result, $V_2 = (4,2) + (30,31) = (31,42), V_3 = (31,42) + (29,44) = (35,9), V_4 = (35,9) + (5,2) = (14,10)$. Then the vertices are $(4,2) \rightarrow A, (31,42) \rightarrow S, (35,9) \rightarrow U$ and $(14,10) \rightarrow N$. Thus, plaintext A SUN successfully received by receiver.

5. Strength Analysis

From matrix theory, we derive key space based on specified parameters. In matrix theory, the set of invertible matrices of order $\zeta \times \zeta$ over the finite field $(\mathbb{F}_p)$, where p is a prime, is represented by the notation $GL_\zeta(\mathbb{F}_p)$. Calculation of the order of the General Linear group (GL_ζ) over the finite field $(\mathbb{F}_p)$ [6] as follows:

$$|GL_\zeta(\mathbb{F}_p)| = (p^\zeta - p^{\zeta-1})(p^\zeta - p^{\zeta-2})(p^\zeta - p^{\zeta-3})\ldots(p^\zeta - p^1)(p^\zeta - 1)$$

The system strength with the recommended key matrix $N^{\theta}_{\alpha,\beta,\zeta}$ over $\mathbb{F}_{41}$ is shown by following table 1.

Table 1

Possible key matrix $N^{\theta}_{\alpha,\beta,\zeta}$ over F_{41}.

ζ	Possible no. of the matrix to check over $\mathbb{F}_{41}$ $\|GL_\zeta(\mathbb{F}_p)\| = (p^\zeta - p^{\zeta-1})(p^\zeta - p^{\zeta-2})(p^\zeta - p^{\zeta-3}).)$ $..(p^\zeta - p^1)(p^\zeta - 1$
	$N^{\theta}_{\alpha,\beta,2} \rightarrow \|GL_2(\mathbb{F}_{41})\| = 2.7552 \times 10^6$
	$N^{\theta}_{\alpha,\beta,3} \rightarrow \|GL_3(\mathbb{F}_{41})\| = 3.192020 \times 10^{14}$
	$N^{\theta}_{\alpha,\beta,4} \rightarrow \|GL_4(\mathbb{F}_{41})\| = 6.21660 \times 10^{25}$
⋮	⋮
ζ	$N^{\theta}_{\alpha,\beta,\zeta} \rightarrow \|GL_\zeta(\mathbb{F}_{41})\| = (41^\zeta - 41^{\zeta-1})(41^\zeta - 41^{\zeta-2})(41^\zeta - 41^{\zeta-3})\ldots(41^\zeta - 41^1)(41^\zeta - 1)$

Clearly shown by preceding table 1, that the prime p huge, then practically it is never be broken". Furthermore, we found that it is independent of θ, α and β and that $GL_\zeta(\mathbb{F}_p)$ increases as key matrix size increases for a fixed p. Hence, it is not feasible to break the system with a Brute-force attack [17, 18, 23], when key space is large. For a fixed p, $GL(\mathbb{F}_p)$ grows as the key matrix's size increases. As a result, when the key area is large, it is not feasible to breach a system using a Brute-force attack [17,18, 23]. The adversary may then try to decipher the cipher text by running it through several statistical tests.

6. Conclusion

In this paper, we have firstly presented a Extended generalized Lucas sequences, which is built using the trace of EGFM(ζ, θ) and we have also determined its initial values. Furthermore, we constructed a recursive matrix with extended generalised Lucas sequences as linear combinations for its entries and examined its non-matrix algebraic properties, including direct calculation of its inverse and product of two matrices, among others. The need for inverse has the field elevated to the status of critical component. Here, we have considered Extended generalised Lucas matrices, which guarantee the existence of an inverse matrix for every element but do not form a multiplicative group EGLM (ζ, θ) for each $(\theta \geq 2) \in \mathbb{N}$ i.e. $N^{\theta}_{\alpha,\beta,\zeta}\, U^{*} = U^{*} N^{\theta}_{\alpha,\beta,\zeta} = I_{\zeta}$, where $U^{*} = N^{-\theta}_{\alpha,\beta,\zeta}\, R^{-1}$. We have also shown how to use Lucas matrices as a key matrix and proposed a new version of public key cryptography that combines the Affine-Hill cypher, Elgamal signature schemes, ECC, and a graph theory approach. The proposed method, which incorporates digital signatures, enhances the system's security: $\zeta, \theta, \alpha, \beta$, and L. Since only Sender and Receiver are aware of U (corresponding to $\zeta, U = N^{(\theta)}_{\alpha,\beta,\zeta}$) and L, it is impossible for anyone to circumvent this system. The proposed solution ensures the correctness and integrity of the data because only Receiver and Sender have access to the keys θ, α, β, and ζ.

References

[1] P. Amudha, J. Jayapriya, and J. Gowri, "An algorithmic approach for encryption using graph labelling," *Journal of Physics*, vol. 1770, no. 1, pp. 012072, 375-384 (2021).

[2] R. Balamurugan, V. Kamalakannan, G. D. Rahul, and S. Tamilselvan, "Enhancing security in text messages using matrix-based mapping and Elgamal method in elliptic curve cryptography," in Proc. International Conference on Contemporary Computing and Informatics (IC3I), IEEE, pp. 103-106 (2014).

[3] V. Billore and N. Patel, "Cryptography utilizing the Affine-Hill cipher and extended generalized Fibonacci matrices," *Electronic Journal of Mathematical Analysis and Applications*, vol. 11, no. 2, pp. 1-12 (2023).

[4] V. Billore, N. Patel, and H. Makwana, "Implementation of extended generalized Fibonacci matrices as a key in modified elliptic curve cryptography," *JP Journal of Algebra, Number Theory and Applications*, vol. 62, no. 2, pp. 123-140 (2023). [Online]. Available: http://dx.doi.org/10.17654/0972555523025.

[5] U. Dixit, "Cryptography: A graph theory approach," *International Journal of Advance Research in Science and Engineering*, vol. 6, no. 01, pp. 218-221 (2017). [Online]. Available: http://www.ijarse.com/images/fullpdf/1504001715BV CNSCS17072DrUmaDixit.pdf

[6] D. S. Dummit and R. M. Foote, *Abstract Algebra*, vol. 3. Hoboken, NJ, USA: Wiley (2004).

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472 (1985).

[8] G. Geetha and P. Jain, "Implementation of matrix-based mapping method using elliptic curve cryptography," *International Journal of Computer Applications Technology and Research*, vol. 3, no. 5, pp. 312-317 (2014).

[9] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*, vol. 1. New York, NY, USA: Springer (2008).

[10] T. Koshy, *Fibonacci and Lucas Numbers with Applications*. Hoboken, NJ, USA: John Wiley & Sons (2019).

[11] M. Kumari and J. Tanti, "On the role of the Fibonacci matrix as key in modified ECC," arXiv (2021). [Online]. Available: https://arxiv.org/abs/2112.11013

[12] P. Mohan, K. Rajendran, and A. Rajesh, "An encryption technique using the adjacency matrices of certain graphs with a self-invertible key matrix," E3S Web of Conf., vol. 376, p. 01108 (2023). [Online]. Available: https://doi.org/10.1051/e3sconf/202337601108

[13] E. Ozkan and I. Altun, "Generalized Lucas polynomials and relationships between the Fibonacci polynomials and Lucas polynomials," *Communications in Algebra*, vol. 47, no. 10, pp. 4020-4030 (2019).

[14] C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Germany: Springer Science & Business Media (2009).

[15] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher," *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 1-12 (2021).

[16] K. Prasad, H. Mahato, and M. Kumari, "A novel public key cryptography based on generalized Lucas matrices," arXiv preprint arXiv:2202.08156v1 (2022).

[17] L. D. Singh and T. Debbarma, "A new approach to elliptic curve cryptography," in Proc. IEEE International Conference on Advanced Communications, Control and Computing Technologies, pp. 78-82 (2014).

[18] S. R. Singh, A. K. Khan, and T. S. Singh, "A critical review on elliptic curve cryptography," in Proc. 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), IEEE, pp. 13-18 (2016).

[19] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Upper Saddle River, NJ, USA: Pearson Education Limited (2017).

[20] P. Stanimirovic, J. Nikolov, and I. Stanimirovic, "A generalization of Fibonacci and Lucas matrices," *Discrete Applied Mathematics*, vol. 156, no. 14, pp. 2606-2619 (2008).

[21] D. R. Stinson, Cryptography: Theory and Practice, 3rd ed. Boca Raton, FL, USA: Chapman and Hall/CRC, Taylor & Francis Group (2006).

[22] P. Sundarayya and G. Vara Prasad, "A public key cryptosystem using affine Hill cipher under modulation of prime number," *Journal of Information and Optimization Sciences*, vol. 40, no. 4, pp. 919-930 (2019).

[23] M. Viswanath and M. R. Kumar, "A public key cryptosystem using Hill's cipher," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, no. 1-2, pp. 129-138 (2015).

[24] W. M. A. Etaiwi, "Encryption algorithm using graph theory," *Journal of Scientific Research and Reports*, vol. 3, no. 19, pp. 2519-2527 (2014).

[25] M. Yamuna, M. Gogia, S. A. Sikka, and M. J. H. Khan, "Encryption using graph theory and linear algebra," *International Journal of Computer Applications*, vol. 2, no. 5, pp. 102-107 (2012).

Received February, 2024