Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 1, pp. 117–129
DOI : 10.47974/JDMSC-2069

A novel multiphase encryption strategy with Fibonacci numbers and matrices

Triveni Domada *
Department of Mathematics
Andhra University Trans-Disciplinary Research Hub
Andhra University
Visakhapatnam 530003
Andhra Pradesh
India

and

Department of Mathematics
Govt. Degree College
Nakkapalli 531081
Anakapalli District
Andhra Pradesh
India

S. Ashok Kumar †
Department of Mathematics
Gayatri Vidya Parishad College for Degree and P. G. Courses (Autonomous)
M. V. P. Colony
Visakhapatnam 530017
Andhra Pradesh
India

Gudela Ashok §
Department of Mathematics
Andhra University Trans-Disciplinary Research Hub
Andhra University
Visakhapatnam 530003
Andhra Pradesh
India

and

* *E-mail:* trivenidomada@gmail.com (Corresponding Author)
† *E-mail:* saiashok.84@gmail.com
§ *E-mail:* ashokavf@gmail.com

Department of Mathematics
Adi Kavi Nannaya University
Rajamahendravaram 533296
Andhra Pradesh
India

D. Chaya Kumari ‡
Department of Mathematics
Gayatri Vidya Parishad College
Rishikonda
Visakhapatnam 530045
Andhra Pradesh
India

Abstract

This paper proposes multiple encryption methods that secures plaintext by integrating various techniques, including the application of graph theory to trees, Fibonacci matrices, and affine transformations. The use of multiple encryption layers minimizes the risks associated with data encryption by ensuring that the compromise of a single layer does not jeopardize the overall security. This multiencryption method can be extended to public key cryptosystems. We introduce a super encryption technique that employs Laplace transformations and Fibonacci numbers. The process begins by applying the Laplace transformation to a selected function, followed by the incorporation of Fibonacci numbers to super encrypt the plaintext. Decryption is achieved by applying the inverse Laplace transform along with the corresponding Fibonacci numbers.

Subject Classification: *Primary 11B39, 05C05, Secondary 44A10.*

Keywords: *Fibonacci matrices, Trees, Laplace transformations, Affine transformations.*

1. Introduction

Cryptography plays a crucial role in ensuring security in computer-based systems by mathematically encrypting and decrypting information. This has applications across various fields, including e-science, e-marketing, and e-business. Super-encryption refers to the process of encrypting data that has already been encrypted. By applying super-encryption multiple times, even relatively weak encryption strategies can be transformed into powerful algorithms.[1][2]

In the modern world, one of the major challenges is security. Ciphers can be represented using graphs to enhance secure communication, and

‡ *E-mail:* **chayakumari.divakarla@gmail.com**

graph theory plays a vital role across various disciplines. Its numerous features and ease of representation as a matrix on computers make graph theory a widely used tool in encryption.

The Fibonacci sequence $\{F_n\}$ can be explained using the recursive relation $F_n = F_{n-2} + F_{n-1}$, $n \geq 2$ where $F_1 = 1$, $F_0 = 0$.

The affine transformation is often referred to as the universal shift cipher, which is a fundamental cryptographic technique. The shift cipher is one of the essential methods used in cryptography. This paper provides an overview of how graph theory is utilized in various studies that explore its applications, along with Fibonacci matrices and affine transformations, in cryptography within the proposed work.[4]

2. Definitions and Standard results

Cryptography: Cryptography is a technique for transmitting messages in a concealed form. The message to be sent is known as "plaintext," while the message that needs to be received in a hidden manner is called "ciphertext." The process of converting understandable plaintext into non understandable ciphertext is known as enciphering, while Deciphering is the process of converting ciphertext back into its original plaintext form.[6]

Types of Cryptography

Symmetric cryptography: In symmetric-key cryptography, the keys used by the sender and the recipient are identical. Consequently, both encryption and decryption procedures requires those keys. These are mostly employed with stream ciphers and block ciphers.[7] [10]

Asymmetric cryptography: Asymmetric cryptography, also known as public-key cryptography, is a method of encryption that uses two separate but mathematically related keys. [7][10]

Laplace transformation: The Laplace transform of a function *f(t),* is denoted with $F(s)$ and is defined for all positive values of t as

$$F(s) = L\{f(t)\} = \int_0^\infty e^{-st} f(t) ds,$$

Whenever the integral value exists with s, a real or complex parameter and Inverse of Laplace Transformation is obtained using the below relation

$$f(t) = L^{-1}\{F(s)\}$$ [18]

Standard results of Laplace transformation:

1. $L\{\cosh at\} = \frac{p}{p^2 - a^2}$, $\quad L^{-1}\left\{\frac{p}{p^2 - a^2}\right\} = \cosh at$
2. $L\{t^n\} = \frac{n!}{p^{n+1}}$ $\quad L^{-1}\left\{\frac{n!}{p^{n+1}}\right\} = t^n$
3. $L\{f^n f(t)\} = \left(-\frac{d}{ds}\right)^n F(s)$ $\quad L^{-1}\left\{\left(-\frac{d}{ds}\right)^n F(s)\right\} = t^n f(t)$ [18][25]

4. Laplace transformation is linear.

   i.e. if $F_1(s) = L\{f_1(t)\}$, $F_2(s) = L\{f_2(t)\}$, $F_3(s) = L\{f_3(t)\}$, ….. $F_n(s) = L\{f_n(t)\}$, then $L\{a_1 f_1(t) + a_2 f_2(t) + \cdots\cdots + a_n f_n(t)\} = a_1 F_1(s) + a_2 F_2(s) + \cdots\cdots + a_n F_n(s)$ where $a_1, a_2, \cdots\cdots, a_n$ are constants

Fibonacci sequence: The sequence 1, 1, 2, 3, 5, 8. . . where each item is created by adding the two former terms, where the initial two terms being 1 and 1. The sequence thus obtained is being referred as the Fibonacci sequence. [3][5][13][15][19][20]

Properties of Fibonacci numbers:

Fibonacci numbers can be obtained using the recursive relation $F_{t+1} = F_t + F_{t-1}$ for $t = 0, 1, 2, \ldots$ The initial values being $F_1 = 1$ and $F_2 = 1$ [3][5][13]

The Fibonacci recurrence relation can be expressed in the matrix form as $\begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix}$, for $n = 2, 3, 4 \ldots$

2nd order Fibonacci matrix is $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$

3rd order Fibonacci matrix is of the form $M_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$; $M_2^{-1} = \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Super Encryption: Super Encryption is the procedure of re-encrypting a message which was currently encrypted one or more times, either using the same method or a new one. Other names for it include multiple encryptions, cascade ciphering, cascade encryption, and super encipherment. The outer-level encryption of a multiple encryption is known as super-encryption [11][16][17]

Multiphase Encryption: Multiphase encryption is a sophisticated approach to securing data by applying multiple layers or phases of

encryption, each using different algorithms, keys, or techniques. This strategy enhances security by making it much more challenging for an unauthorized party to decrypt the data, even if they manage to break one layer of encryption.[11][14][16][17]

Graph: Mathematically a graph represents a network, it describes the relationships between discrete objects.[4][8][9]

Directed Graph: A graph with edges having a specific direction, indicating the relationship between two vertices flows from one vertex to another is termed as a directed graph.[4][8][9][12]

Un Directed Graph: A graph with edges having no specific direction is known as an undirected graph.[4][8][9][12]

Connected Graph: In a connected graph, we can travel from any vertex to any other vertex by traversing edges.[4][8][9][12][21][22]

Tree: A tree is a graph that does not have cycles but has a single path connecting any two vertices.

Binary Tree: If every vertex has an out-degree of two or less, a rooted tree is referred to as a binary tree.[21][22]

Weighted tree: A tree is referred to as a weighted tree if each leaf or edge is given a positive integer. [21][22]

Optimal tree: Optimal tree is one of many weighted trees that can exist for a given set of weights. The tree in this collection with the lowest weight is referred to as the optimum tree.[4][8][9][12][21][22]

Code: A code is a binary string of digits that are assigned to each letter in a message (0s and 1s).[12]

3. Algorithm

3.1 *Algorithm for Method1: Multiphase encryption of Laplace Transformation via Fibonacci Numbers*

Encryption:

Step 1: Choose the message $P_0, P_1, P_2, ...P_m$ and converted into ASCII code integer $M_0, M_1, ...M_m$ Consider the function $f(t) = t\sin t$ with $t\sin t = t^2 - \frac{t^4}{3!} + \frac{t^6}{5!} - \frac{t^8}{7!} + \frac{t^{10}}{9!} - \frac{t^{12}}{11!} + \frac{t^{14}}{13!} - \frac{t^{16}}{15!} + \frac{t^{18}}{17!}$ and apply Laplace transformation on both sides.

Step 2: Then, write $M_0, M_1, ...M_m$ as the coefficients of the expansion of $t\sin t$ and evaluate $M_0, M_1, ...M_m$ mod26 and send the multiples as public key.

Step 3: Now, add that Fibonacci number to the remainder of $M_0, M_1, ...M_m$ (mod26) as super encryption

Step 4: Send the super encrypted message as $Q_0, Q_1, ...Q_m$ and Exchange the Fibonacci numbers as private key.

Decryption:

Step 1: Take $Q_0, Q_1, ...Q_m$ and subtracted the Fibonacci numbers which are exchanged privately and get $R_0, R_1, ...R_m$ as first level of decryption

Step 2: By using the public key we can decrypt the message

Step 3: Apply inverse Laplace transformation to get decrypted message

Step 4: Apply ASCII code to get the original plain text.

Example:

Encryption:

Message to be sent is HABITATION

H	A	B	I	T	A	T	I	O	N
7	0	1	8	19	0	19	8	14	13

In ASCII code

104	97	98	105	116	97	116	105	111	110

$$\sin t = t - \frac{t^3}{3!} + \frac{t^5}{5!} - \frac{t^7}{7!} + \frac{t^9}{9!} - \frac{t^{11}}{11!} + \frac{t^{13}}{13!} - \frac{t^{15}}{15!} + \frac{t^{17}}{17!} - \frac{t^{19}}{19!}$$

$$t\sin t = t^{1+1} - \frac{t^{3+1}}{3!} + \frac{t^{5+1}}{5!} - \frac{t^{7+1}}{7!} + \frac{t^{9+1}}{9!} - \frac{t^{11+1}}{11!} + \frac{t^{13+1}}{13!} - \frac{t^{15+1}}{15!} + \frac{t^{17+1}}{17!} - \frac{t^{19+1}}{19!}$$

$$t\sin t = 104t^2 - 97\frac{t^4}{3!} + 98\frac{t^6}{5!} - 105\frac{t^8}{7!} + 116\frac{t^{10}}{9!} - 97\frac{t^{12}}{11!} + 116\frac{t^{14}}{13!} - 105\frac{t^{16}}{15!} + 111\frac{t^{18}}{17!} - 110\frac{t^{20}}{19!}$$

$$L\{t\sin t\} = L\{104t^2 - 97\frac{t^4}{3!} + 98\frac{t^6}{5!} - 105\frac{t^8}{7!} + 116\frac{t^{10}}{9!} - 97\frac{t^{12}}{11!} + 116\frac{t^{14}}{13!} - 105\frac{t^{16}}{15!} + 111\frac{t^{18}}{17!} - 110\frac{t^{20}}{19!}\}$$

$$\frac{2s}{(s^2+1)^2} = 104\frac{2!}{s^{2+1}} - \frac{97}{3!}\frac{4!}{s^{4+1}} + \frac{98}{5!}\frac{6!}{s^{6+1}} - \frac{105}{7!}\frac{8!}{s^{8+1}} + \frac{116}{9!}\frac{10!}{s^{10+1}} - \frac{97}{11!}\frac{12!}{s^{12+1}} + \frac{116}{13!}\frac{14!}{s^{14+1}} - \frac{105}{15!}\frac{16!}{s^{16+1}} + \frac{111}{17!}\frac{18!}{s^{18+1}} - \frac{110}{19!}\frac{20!}{s^{20+1}}$$

$$\frac{2s}{(s^2+1)^2} = \frac{208}{s^{2+1}} - \frac{388}{s^{4+1}} + \frac{588}{s^{6+1}} - \frac{840}{s^{8+1}} + \frac{1160}{s^{10+1}} - \frac{1164}{s^{12+1}} + \frac{1624}{s^{14+1}} - \frac{1680}{s^{16+1}} + \frac{1998}{s^{18+1}} - \frac{2200}{s^{20+1}}$$

$$q_0 = 208, q_1 = 388, q_2 = 588, q_3 = 840, q_4 = 1160, q_5 = 1164, q_6 = 1624,$$

$$q_7 = 1680, q_8 = 1998, q_9 = 2200$$

$$x_0 = 26\times 8 + 0, x_1 = 26\times 14 + 24, x_2 = 26\times 22 + 16, x_3 = 26\times 32 + 8$$

$$x_4 = 26\times 44 + 16, x_5 = 26\times 44 + 20, x_6 = 26\times 62 + 12, x_7 = 26\times 64 + 16$$

$$x_8 = 26\times 76 + 22, x_9 = 26\times 84 + 16$$

Public Key is : 8,14,22,32,44,44,62,64,76,84
Second level encryption with Fibonacci Numbers

$0 + F_0 = 1 \bmod 26 = 1,$ $24 + F_{24} = 46392 \bmod 26 = 8,$
$16 + F_{16} = 1003 \bmod 26 = 15,$ $8 + F_8 = 29 \bmod 26 = 3$
$16 + F_{16} = 1003 \bmod 26 = 15,$ $20 + F_{20} = 6785 \bmod 26 = 25$
$12 + F_{12} = 156 \bmod 26 = 0,$ $16 + F_{16} = 1003 \bmod 26 = 15$
$22 + F_{22} = 17733 \bmod 26 = 1,$ $16 + F_{16} = 1003 \bmod 26 = 15$

Key is: $F_0, F_{24}, F_{16}, F_8, F_{16}, F_{20}, F_{12}, F_{16}, F_{22}, F_{16}$

Encrypted Message is: 1, 8, 15, 3, 15, 25, 6, 15, 1, 15
: B I P D P Z G P B P

Decryption:

The message to be decrypted is B I P D P Z G P B P
Numerical equivalent is 1, 8, 15, 3, 15, 25, 6, 15, 1, 15

$$1 - F_0 (\bmod 26) = 0$$
$$8 - F_{24} (\bmod 26) = -46360 (\bmod 26) = 24$$
$$15 - F_{16} (\bmod 26) = -972 (\bmod 26) = 16$$
$$3 - F_8 (\bmod 26) = -18 (\bmod 26) = 8$$

$$15 - F_{16} (\text{mod}\, 26) = -972 (\text{mod}\, 26) = 16$$
$$25 - F_{20} (\text{mod}\, 26) = -6740 (\text{mod}\, 26) = 20$$
$$0 - F_{12} (\text{mod}\, 26) = -144 (\text{mod}\, 26) = 12$$
$$15 - F_{16} (\text{mod}\, 26) = -972 (\text{mod}\, 26) = 16$$
$$1 - F_{22} (\text{mod}\, 26) = -17710 (\text{mod}\, 26) = 22$$
$$15 - F_{16} (\text{mod}\, 26) = -972 (\text{mod}\, 26) = 16$$

Second level decryption using public key:

$$x_0 = 26 \times 8 + 0, x_1 = 26 \times 14 + 24, x_2 = 26 \times 22 + 16, x_3 = 26 \times 32 + 8$$

$$x_4 = 26 \times 44 + 16, x_5 = 26 \times 44 + 20, x_6 = 26 \times 62 + 12, x_7 = 26 \times 64 + 16$$

$$x_8 = 26 \times 76 + 22, x_9 = 26 \times 84 + 16$$

$$\frac{2s}{(s^2+1)^2} = \frac{208}{s^{2+1}} - \frac{388}{s^{4+1}} + \frac{588}{s^{6+1}} - \frac{840}{s^{8+1}} + \frac{1160}{s^{10+1}} - \frac{1164}{s^{12+1}} + \frac{1624}{s^{14+1}} - \frac{1680}{s^{16+1}} + \frac{1998}{s^{18+1}} - \frac{2200}{s^{20+1}}$$

$$\frac{2s}{(s^2+1)^2} = 104 \frac{2!}{s^{2+1}} - \frac{97}{3!} \frac{4!}{s^{4+1}} + \frac{98}{5!} \frac{6!}{s^{6+1}} - \frac{105}{7!} \frac{8!}{s^{8+1}} + \frac{116}{9!} \frac{10!}{s^{10+1}} - \frac{97}{11!} \frac{12!}{s^{12+1}} +$$
$$\frac{116}{13!} \frac{14!}{s^{14+1}} - \frac{105}{15!} \frac{16!}{s^{16+1}} + \frac{111}{17!} \frac{18!}{s^{18+1}} - \frac{110}{19!} \frac{20!}{s^{20+1}}$$

$$L\{t \sin t\} = L\{104t^2 - 97 \frac{t^4}{3!} + 98 \frac{t^6}{5!} - 105 \frac{t^8}{7!} + 116 \frac{t^{10}}{9} - 97 \frac{t^{12}}{11!} + 116 \frac{t^{14}}{13!} -$$
$$105 \frac{t^{16}}{15!} + 111 \frac{t^{18}}{17!} - 110 \frac{t^{20}}{19!}\}$$

$$t \sin t = 104t^2 - 97 \frac{t^4}{3!} + 98 \frac{t^6}{5!} - 105 \frac{t^8}{7!} + 116 \frac{t^{10}}{9} - 97 \frac{t^{12}}{11!} + 116 \frac{t^{14}}{13!} -$$
$$105 \frac{t^{16}}{15!} + 111 \frac{t^{18}}{17!} - 110 \frac{t^{20}}{19!}$$

Take the co efficient of the above-mentioned finite polynomial and label them as

$$R_0 = 104, R_1 = 97, R_2 = 98, R_3 = 105, R_4 = 116, R_5 = 97, R_6 = 116, R_7 = 105,$$
$$R_8 = 111, R_9 = 110$$

The final decrypted message can be obtained using ASCII codes and the message is **HABITATION**

3.2 *Algorithm for Method 2: Multiphase encryption of Trees via Fibonacci Matrices*

Encryption Procedure:

Step 1: Take the plain text P and convert it into numerical equivalent.

Step 2: Using Huffman's method and the aforementioned numerical equivalents, draw an optimal tree.

Step 3: Write prefix codes of letter in the form of a matrix and multiply it with suitable ordered Fibonacci Matrix to get the second level cipher text.

Step 4: Again, encrypt the text obtained in previous step with Affine to get final cipher text.

Decryption Procedure:

Step 1: Inverse affine transformation is used as the initial step of decryption by the receiver after receiving the cypher text from the sender.

Step 2: In second level, the text can be decrypted by multiplying the text in matrix form with

Inverse Fibonacci matrix, which is shared as a secret key.

Step 3: With the private key the sender sent, the recipient now develops his own optimal tree to retrieve the plain text.

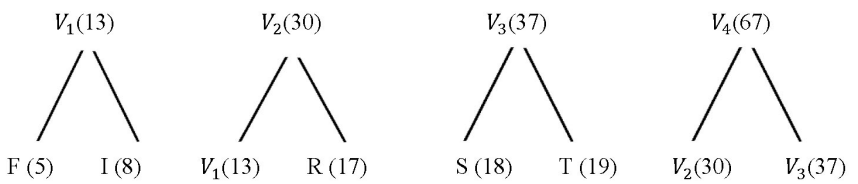
Example:

Encryption:

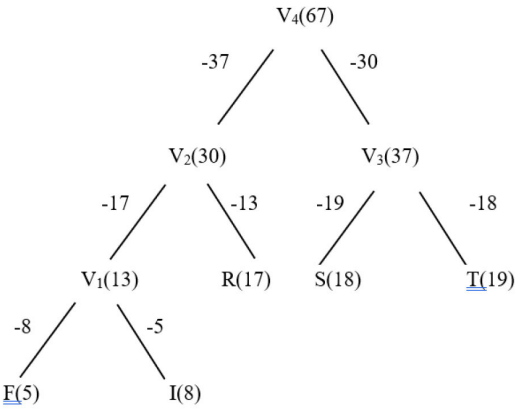
Message to be sent is FIRST

F	I	R	S	T
5	8	17	18	19

First level encryption:



Construct optimal weighted tree corresponding to the given message using the binary trees constructed above.



Optimal Weighted Tree

Second level encryption:
Matrix representation of the optimal weighted tree is

$$M_1 = \begin{bmatrix} -37 & -17 & -8 \\ -37 & -17 & -5 \\ -37 & -13 & 0 \\ -30 & -19 & 0 \\ -30 & -18 & 0 \end{bmatrix}$$

From the 3×3 Fibonacci Matrix we have $M_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$; $M_2^{-1} = \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$$C = M_1 M_2 = \begin{bmatrix} -37 & -17 & -8 \\ -37 & -17 & -5 \\ -37 & -13 & 0 \\ -30 & -19 & 0 \\ -30 & -18 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -17 & -54 & -45 \\ -17 & -54 & -42 \\ -13 & -50 & -37 \\ -19 & -49 & 0 \\ -18 & -48 & 0 \end{bmatrix}$$

Third Level Encryption:
Using the transformation as $y = ax + b(\mathrm{mod}\,26)$ with $a = 5,\ b = 14$

x	-17	-54	-45	-17	-54	-42	-13	-50	-37	-19	-49	0	-18	-48	0
$5x + 14$	-71	-256	-211	-71	-256	-196	-51	-236	-171	-81	-231	14	-76	-226	14
mod 26	7	4	23	7	4	12	1	24	11	23	3	14	2	8	14
y	H	E	X	H	E	M	B	Y	L	X	D	O	C	I	O

The final cypher text is: HEXHEMBYLXDOCIO

Decryption:

Level 1: The receiver applies inverse Affine Transformation $msg = a^{-1}(y-b)(\text{mod}26)$

With $a = 5 \Rightarrow a^{-1} = 21 \bmod 26$ and $b = 5$

y	7	4	23	7	4	12	1	24	11	23	3	14	2	8	14
$y-14$	-7	-10	9	-7	-10	-2	-13	10	-3	9	-11	0	-12	-6	0
$21(y-14)$	-147	-210	189	-147	-210	-42	-273	210	-63	189	-231	0	-252	-126	0
Mod 26	-17	-54	-45	-17	-54	-42	-13	-50	-37	-19	-49	0	-18	-48	0

Equivalent matrix representation is

$$C = \begin{bmatrix} -17 & -54 & -45 \\ -17 & -54 & -42 \\ -13 & -50 & -37 \\ -19 & -49 & 0 \\ -18 & -48 & 0 \end{bmatrix}$$

$$\text{Now } P = C \times M_2^{-1} = \begin{bmatrix} -17 & -54 & -45 \\ -17 & -54 & -42 \\ -13 & -50 & -37 \\ -19 & -49 & 0 \\ -18 & -48 & 0 \end{bmatrix} \times \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -37 & -17 & -8 \\ -37 & -17 & -5 \\ -37 & -13 & 0 \\ -30 & -19 & 0 \\ -30 & -18 & 0 \end{bmatrix}$$

Finally, the receiver will construct the optimal tree using the private key that has been shared

5. Conclusion

The proposed cryptosystems offer greater security compared to symmetric cryptosystems and can generate multiple passwords. Additionally, they can be adapted for use in public key cryptosystems

References

[1] A. N. Philippou, A. F. Horadan, and G. E. Bergun, *Application of Fibonacci Numbers*, Springer Science Media LLC.

[2] S. Babu, "Modification affine ciphers algorithm for cryptography password," *Int. J. Res. Sci. Eng.*, vol. 3, no. 2, pp. 346-351 (2017).

[3] J. B. Bacani and J. F. T. Rabago, "On generalized Fibonacci numbers," arXiv preprint arXiv:1503.05305 (2015).

[4] B. Kittur, D. C. Kumari, S. G. Kulkarni, and M. K. M, "Super-encryption method using affine transform via trees," *International Journal of Mathematics Trends and Technology*, vol. 68, no. 6 (2022).

[5] D. C. Kumari and S. Ashok Kumar, "Redei rational functions as permutation function and an algorithm to compute Redei rational functions," *International Journal of Engineering, Science and Mathematics*, vol. 8, no. 2, pp. 2320-0294, Feb. (2019).

[6] F. Piper and S. Murthy, *Cryptography: A Very Short Introduction*.

[7] G. Ashok, S. Ashok Kumar, D. C. Kumari, and M. Ramakrishna, "A type of public cryptosystem using polynomials and Pell sequences," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 7, pp. 1951-1963 (2022). doi: 10.1080/09720529.2022.2133237.

[8] J. S. Han, H. S. Kim, and J. Neggers, "On Fibonacci functions with Fibonacci numbers," *Advances in Difference Equations*, pp. 1-7 (2012).

[9] T. C. Hu and K. C. Tan, "Path length of binary search trees," *SIAM Journal on Applied Mathematics*, vol. 22, no. 2, pp. 225-234 (1972).

[10] J. Buchman, *Introduction to Cryptography*, Springer-Verlag (2001).

[11] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 8, pp. 2341-2352 (2022). doi: 10.1080/09720529.2020.1838744.

[12] R. Klein and D. Wood, "On the path length of binary trees," *Journal of the ACM (JACM)*, vol. 36, no. 2, pp. 280-289 (1989).

[13] K. H. Rosen, *Elementary Number Theory and Its Applications*, 3rd ed., Addison-Wesley.

[14] Y. S. Mezaal and S. F. Abdulkareem, "Affine cipher cryptanalysis using genetic algorithms," *JP Journal of Algebra, Number Theory and Applications*, vol. 39, no. 5, pp. 785-802 (2017).

[15] N. Koblitz, *A Course in Number Theory and Cryptography*, ISBN 3-578071-8, SPIN 10893308.

[16] S. A. Kumar, A. Chandra Sekhar, C. Pragathi, and B. Ravi Kumar, "Multiple encryption of various ciphers," *International Journal of Engineering Science Invention Research & Development*, vol. II, no. VIII, Feb. (2016).

[17] S. A. Kumar, A. Chandra Sekhar, and D. C. Kumari, "Symmetric key cryptosystem for multiple encryptions," *International Journal of Mathematics Trends and Technology (IJMTT)*, vol. 29, no. 2, pp. 140-144, Jan. (2016). ISSN: 2231-5373.

[18] H. Sheng, Y. Li, and Y. Q. Chen, "Application of numerical inverse Laplace transform algorithms in fractional calculus," *Journal of the Franklin Institute*, vol. 348, no. 2, pp. 315-330 (2011).

[19] S. L. Basin, "Generalized Fibonacci sequences and squared rectangles," *The American Mathematical Monthly*, vol. 70, no. 4, pp. 372-379 (1963).

[20] T. Khoshy, "Fibonacci, Lucas, and Pell numbers and Pascal's triangle," *Applied Probability Trust*, pp. 125-132.

[21] T. Domada, S. A. Kumar, G. Ashok, and D. C. Kumari, "Super-encryption with Pell-Lucas matrices and graphs via Laplace transformations," *Journal of Harbin Engineering University*, vol. 44, no. 8, pp. 8975-980 (2023).

[22] T. Domada, S. A. Kumar, G. Ashok, and D. C. Kumari, "Super-encryption technique of graphs via matricial approach," *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 1215-1222, Jun. 26 (2024). doi: 10.47974/JDMSC-1976.

Received November, 2023