Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 8
August 2023

Super-Encryption with Pell-Lucas Matrices and Graphs via Laplace Transformations

Triveni Domada [1,2*], S. Ashok Kumar [4], Gudela Ashok[1,3], D. Chaya Kumari [4]

[1]Research Scholar, Department of Mathematics, Andhra University TDR Hub.

[2]Lecturer in Mathematics, Dr. V. S. Krishna Govt. Degree College (A), Visakhapatnam.

[3]Assistant Professor, Department of Mathematics, Adikavi Nannaya University.

[4]Assistant Professor, Gayatri Vidya Parishad College for Degree and P. G. Courses(A).
trivenidomada@gmail.com*

Abstract

This research study suggests a novel encryption method called multiphase encryption. Multiphase encryption method encrypts the original data multiple times using various powerful encryption algorithms at each stage. Multiphase encryption method using graph theory properties of trees, Pell-Lucas Matrices and Vigenère cipher greatly increases the complexity of the encryption algorithm and another a new technique of super encryption using Laplace transformations through Fibonacci numbers by exploiting the properties of trees in graph theory via Beaufort cipher to encrypt the plain text which is more secure than the symmetric key cryptosystem as the plain text is encrypted in multi layers.

Keywords- Cryptography, Beaufort Transformations, Laplace Transformations, tree, Vigenère cipher, Pell-Lucas Matrix.

1 Introduction

In today's digital age, data security stands as a paramount concern in safeguarding sensitive information from unauthorized access. The conventional methods of encryption have served as a robust defence mechanism against cyber threats, yet the ever-evolving landscape of technology necessitates the continuous development of more intricate encryption techniques. This research study introduces a ground-breaking approach to encryption - the Multiphase Encryption Method - designed to fortify data protection through the fusion of graph theory, mathematical matrices, and historical ciphers.

1.1 The Need for Enhanced Data Security:

As our reliance on digital communication and data storage deepens, the potential risks posed by cyberattacks become increasingly evident. Traditional encryption mechanisms, while effective, may face challenges in ensuring fool proof security against the relentless efforts of malicious entities. This highlights the urgency for encryption methodologies that not only withstand present-day cryptographic challenges but also anticipate and thwart potential future threats.

1.2 Introducing Multiphase Encryption:

The core premise of the Multiphase Encryption Method lies in its multifaceted approach to data protection. Rather than relying solely on a single encryption algorithm, this novel approach applies a cascade of powerful encryption techniques, reinforcing the security layers enveloping the original data. By implementing a multi-stage encryption process, each subsequent layer of encryption enhances the complexity of deciphering, rendering unauthorized access an immensely arduous task.

1.3 Leveraging Graph Theory and Mathematical Matrices:

A distinctive aspect of this research lies in its integration of graph theory properties, Pell-Lucas matrices, and Vigenère cipher into the encryption process. Graph theory, a field of mathematics concerned with the study of interconnected

nodes, contributes to the development of intricate encryption pathways akin to tree structures. Pell-Lucas matrices provide a mathematical foundation for generating complex sequences, thereby introducing an element of mathematical unpredictability into the encryption scheme.

1.4 Super Encryption via Mathematical Ciphers:
To further bolster data security, this research introduces a new technique called "super encryption" using Laplace transformations and Fibonacci numbers. By capitalizing on the inherent properties of trees within graph theory, this technique combines with the Beaufort cipher to encrypt plaintext data. This approach creates multiple layers of encryption that are challenging to decipher, ultimately exceeding the security offered by traditional symmetric key cryptosystems.

2 Definitions
Laplace Transformation: Let f(t) be a function of a real variable t, defined for all t>0, then Laplace transform of f(t) is denoted with L{f(t)} and is defined as
L{f(t)}=F(s) provided the integral exists, where "s" is real or complex.
Few results of Laplace Transform:
If $L\{f_i(t)\}= F_i(s)$ for $1\leq i\leq n$ then
$L\{a_0 f_0(t)+ a_1 f_1(t)+\ldots+ a_n f_n(t)\} = a_0F_0(s)+ a_1F_1(s)+ \ldots + a_nF_n(s)$,
$L\{\cosh kt\} = \frac{s}{s^2-k^2}$, $L^{-1}\{\frac{s}{s^2-k^2}\} = \cosh kt$
$L\{t^n\}=\frac{n!}{s^{n+1}}$, $L^{-1}\{\frac{n!}{s^{n+1}}\} =t^n$
$L\{f^{(n)}(t)\}=(-\frac{d}{ds})^nF(s)$, $L^{-1}\{(-\frac{d}{ds})^nF(s)\}= f^n(t)$,

And the inverse Laplace transform is defined as $L^{-1}\{F(s)\}=f(t)$.

2.1 Graph: Mathematically a graph represents a network, it describes the relationships between discrete objects

2.2 Directed Graph: A directed graph is graph in which a set of vertices that are connected together, where all the edges are directed from one vertex to another.

2.3 Un Directed Graph: An undirected graph is graph in which a set of vertices that are connected together, In an undirected graph the edges are bidirectional.

2.4 Connected Graph: An undirected graph with a path between every pair of vertices is called a connected graph.

2.5 Tree: A tree is a graph that does not have cycles but has a single path connecting any two vertices.
2.6 Binary Tree: If every vertex has an out-degree of two or less, arooted tree is referred to as a binary tree.

2.7 Weighted tree: A tree is referred to as a weighted tree if each leaf or edge is given a positive integer.

2.8 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.

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

2.10 Prefix code: A set S of binary sequences is said to be a prefix code if any of the binary sequences in that set do not appear at the beginning of the binary sequence of any other code.

2.11 Cryptography: The method of conveying messages while maintaining secrecy is known as cryptography.

2.12 Plain Text: Messages or information to be conveyed by the sender to the recipient are referred to as plain text.

2.13 Cipher text: A message that has been encoded or encrypted and contains plain text but in an unintelligible format is referred to as cypher text.

There are two varieties of encryption.

2.14 Symmetric key Cryptography: Using the same key for both encryption and decryption is known as symmetric key cryptography.

2.15 Asymmetric key Cryptography: Using different keys for encryption and decryption is known as asymmetric key cryptography.

2.16 Beaufort cipher: The Beaufort cipher is a simple polyalphabetic cipher. It makes use of the tabula recta table.
Super Encryption: Super encryption is the process of encrypting a message that has previously been encrypted. It is a means to secure data by combining two or more cryptographic algorithms.
2.17 Pell-Lucas numbers: Pell-Lucas Numbers defined using the recursive relation
$Q_n = Q_{n-2} + 2Q_{n-1}$, for $n = 2,3,4, \ldots$
with initial values $Q_0 = Q_1 = 2$
Also, the n^{th} Pell-Lucas Numbers are given by the following formulas
Binet-type relation $Q_n = (1+\sqrt{2})^n + (1-\sqrt{2})^n$
Binomial sum of the type $Q_n = 2\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} 2^k$
It is also observed that for a Pell-Lucas number $Q_n/2$ is a prime, which requires the condition that n either a power of 2 or a prime.
First few Pell-Lucas Numbers are given by 2,2,6,14,34,82,198,478,1154,…
Pell-Lucas numbers can be written in the form a matrix and 3×3 matrix can be taken as

$$M_2 = \begin{bmatrix} Q_2 & Q_1 & 0 \\ Q_1 & Q_0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

[12][13][14][15][16]

2.18 Vigenère cipher: The Vigenère cipher is one technique for encrypting alphabetic text, which employs a basic polyalphabetic substitution approach. The term "polyalphabetic cypher" refers to any substitution-based cypher that makes use of a variety of substitution alphabets. The source text is secured using the Vigenère square or Vigenère table.[17][18][19][20]

3 Multiple Encryption Method Using Laplace Transformations and Trees Proposed Encryption & Decryption Algorithms

For Encryption:

Step1: Choose the message $M_0,M_1,M_2,\ldots,M_n$

Consider the function $f(t)= t\ sint$ with

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

Step 2: Write $M_0,M_1,M_2,\ldots,M_n$ as coefficients, apply Laplace Transformation on both sides of the above equation, apply mod 26 and use the multiples as public key1.

Remainders are $R_0, R_1, R_2,\ldots, R_n$.

Step 3: Use Huffman's procedure to draw an optimal tree for $R_0, R_1, R_2,\ldots, R_n$ and Prefix codes of the letters acquired as leaves in the ideal tree were translated to decimal equivalents.

Step 4: Add decimal equivalent obtained in previous step to the level of each leaf apply mod 26, use the multiples as public key2 and send this as cipher text, secret key is the level of each tree.

Step 5: Again, encrypt this message using Beaufort cipher.

For Decryption:

Step1: Decrypt the cipher text with Beaufort decryption cipher in first level of decryption using public key2.

Step2: As a second level of decryption, apply secret (private key-level) to the decrypted cypher text.

Step3: Subtract the ideal tree levels from the decrypted text's numerical equivalents.

Step4: Decrypted message can be obtained on applying Inverse Laplace Transform.

4 Example

Encryption:

Consider the word

C	O	N	F	I	D	E	N	C	E
2	14	13	5	8	3	4	13	2	4

First level Encryption:

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

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

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

$$L\{t\sin t\} = 2\frac{2!}{s^3} - \frac{14}{3!}\frac{4!}{s^5} + \frac{13}{5!}\frac{6!}{s^7} - \frac{5}{7!}\frac{8!}{s^9} + \frac{8}{9!}\frac{10!}{s^{11}} - \frac{3}{11!}\frac{12!}{s^{13}} + \frac{4}{13!}\frac{14!}{s^{15}} - \frac{13}{15!}\frac{16!}{s^{17}} + \frac{2}{17!}\frac{18!}{s^{19}} - \frac{4}{19!}\frac{20!}{s^{21}}$$

$$L\{t\sin t\} = 4\frac{1}{s^3} - 56\frac{1}{s^5} + 78\frac{1}{s^7} - 40\frac{1}{s^9} + 80\frac{1}{s^{11}} - 36\frac{1}{s^{13}} + 56\frac{1}{s^{15}} - 208\frac{1}{s^{17}} + 36\frac{1}{s^{19}} - 80\frac{1}{s^{21}}$$

q_0=4, q_1=56, q_2=78, q_3=40, q_4=80, q_5=36, q_6=56, q_7=208, q_8=36, q_9=80

$$x_0 = 26\times 0 + 4 \qquad x_1 = 26\times 2 + 4$$

$$x_2 = 26\times 3 + 0$$

$$x_3 = 26\times 1 + 14 \qquad x_4 = 26\times 3 + 2$$

$$x_5 = 26\times 1 + 10$$

$$x_6 = 26\times 2 + 4 \qquad x_7 = 26\times 8 + 0$$

$$x_8 = 26\times 1 + 10$$

$$x_9 = 26\times 3 + 2$$

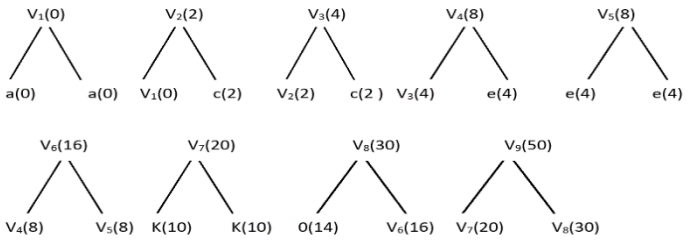
Public Key 1: 0,2,3,1,3,1,2,8,1,3

First Level Cipher Text: 4,4,0,14,2,10,4,0,10,2

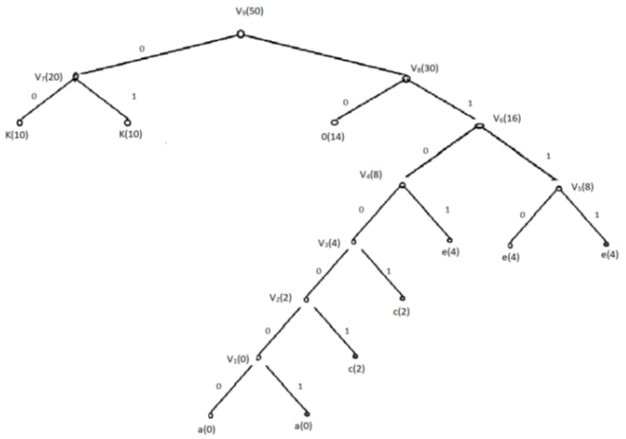
: e,e,a,o,c,k,e,a,k,c

In ascending order : a,a,c,c,e,e,e,k,k,o

a	a	c	c	e	e	e	k	k	o
0	0	2	2	4	4	4	10	10	14



Optimal Tree



Second level of Encryption:
Table:

Alphabets	e	e	a	o	c	k	e	a	k	c
Binary	1101	1110	1100000	10	110001	00	1111	1100001	01	11001
Decimal	13	14	96	2	49	0	15	97	1	25
Level	4	4	7	2	6	2	4	7	2	5
Decimal+Level	17	18	103	4	55	2	19	104	3	30
Mod26	17	18	25	4	3	2	19	0	3	4
Cipher Text	r	s	z	e	d	c	t	a	d	e

Key2: 0 0 3 0 2 0 0 4 0 1
Second Level Cipher Text : r s z e d c t a d e

Third level of Encryption:
Plain Text : r s z e d c t a d e
Beaufort cipher with key3 : c r a z y c r a z y
Final Level Cipher Text : l z b v v a y a w u

Decryption:
Using the cypher text "lzbvvayawu" obtained in final level, Plain Text for third level can be obtained by applying Beaufort cipher for decryption with Key crazy.
Final Level Cipher Text : l z b v v a y a w u
Using Beaufort cipher decryption
key3 :c r a z y c r a z y
Plain Text : r s z e d c t a d e
Now for second level subtract level from decimal equivalent after decrypting using Public key 2.

Cipher Text	r	s	z	e	d	c	t	a	d	e
Decimal	17	18	25	4	3	2	19	0	3	4
Decimal with public key2	17	18	103	4	55	2	19	104	3	30
Level	4	4	7	2	6	2	4	7	2	5
Decimal-Level	13	14	96	2	49	0	15	97	1	25
Binary	1101	1110	1100000	10	110001	00	1111	1100001	01	11001
Level2 cipher Text	e	e	a	o	c	k	e	a	k	c

For final level of decryption use Public Key 1.

$$x_0 = 26\times 0+4 \qquad x_1 = 26\times 2+4$$
$$x_2 = 26\times 3+0$$
$$x_3 = 26\times 1+14 \qquad x_4 = 26\times 3+2$$
$$x_5 = 26\times 1+10$$
$$x_6 = 26\times 2+4 \qquad x_7 = 26\times 8+0$$
$$x_8 = 26\times 1+10$$
$$x_9 = 26\times 3+2$$

$$\frac{2s}{(s^2+1)^2} =$$

$$4\frac{1}{s^3}-56\frac{1}{s^5}+78\frac{1}{s^7}-40\frac{1}{s^9}+80\frac{1}{s^{11}}-36\frac{1}{s^{13}}+56\frac{1}{s^{15}}-208\frac{1}{s^{17}}+36\frac{1}{s^{19}}-80\frac{1}{s^{21}}$$

$$L^{-1}\left\{\frac{2s}{(s^2+1)^2}\right\} =$$

$$L^{-1}\left\{\frac{4}{s^3}\right\}-L^{-1}\left\{\frac{56}{s^5}\right\}+L^{-1}\left\{\frac{78}{s^7}\right\}-L^{-1}\left\{\frac{40}{s^9}\right\}+L^{-1}\left\{\frac{80}{s^{11}}\right\}-L^{-1}\left\{\frac{36}{s^{13}}\right\}+$$

$$L^{-1}\left\{\frac{56}{s^{15}}\right\}-L^{-1}\left\{\frac{208}{s^{17}}\right\}+L^{-1}\left\{\frac{36}{s^{19}}\right\}-L^{-1}\left\{\frac{80}{s^{21}}\right\}$$

t sint=

$$4\frac{t^2}{2!}-56\frac{t^4}{4!}+78\frac{t^6}{6!}-40\frac{t^8}{8!}+80\frac{t^{10}}{10!}-36\frac{t^{12}}{12!}+56\frac{t^{14}}{14!}-208\frac{t^{16}}{16!}+36\frac{t^{18}}{18!}-80\frac{t^{20}}{20!}$$

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

Now take the sequence of coefficients (only magnitude)
a_0=2, a_1=14, a_2=13, a_3=5, a_4=8, a_5=3, a_6=4, a_7=13, a_8=2, a_9=4.
and the plain text will be CONFIDENCE whose decimal equivalent is the sequence
2 14 13 5 8 3 4 13 2 4

5 A Type of Multiphase Encryption System Using Graph Theory and Pell-Lucas Matrices

Steps for Encryption:
Step1: Consider the message P and transform it to it numerical equal value.
Step2: Draw a suitable optimal tree with Huffman's approach and the aforementioned numerical equivalents.
Step3: To create the second level cypher text, write the letter prefix codes as a matrix and multiply them with the appropriate ordered Pell-Lucas matrix.
Step4: Finally, encrypt the text obtained in previous step using Vigenère cipher to get the final cipher text.

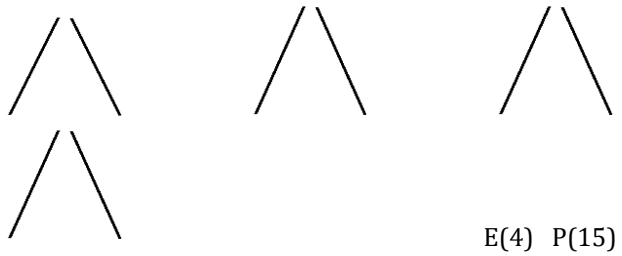
Steps for Decryption:
Step1: The receiver uses inverse Vigenère cipher as the first phase of decryption after receiving the encrypted text from the sender.
Step2: By multiplying the text in matrix form with the Inverse Pell-Lucas matrix, which is used as a shared secret key, the text can be decoded at the second level.
Step3: The recipient now creates his own optimum tree using the private key the sender sent. Then the plain text will be retrieved.

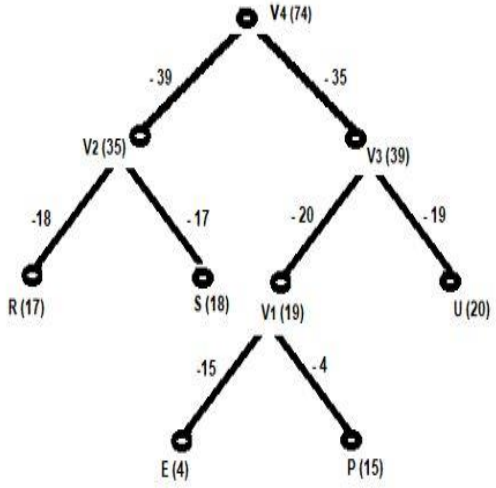
6 EXAMPLE

S	U	P	E	R
18	20	15	4	17

E	P	R	S	U
4	15	17	18	20

$V_1(19)$ $V_2(35)$ $V_3(39)$ $V_4(74)$





Optimal Tree

Matrix representation is $M_1=\begin{bmatrix}-39 & -18 & 0\\ -39 & -17 & 0\\ -35 & -20 & -15\\ -35 & -20 & -4\\ -35 & -19 & 0\end{bmatrix}$

Let us consider 3×3 Pell Lucas matrix of the form $M_2 = \begin{bmatrix}Q_2 & Q_1 & 0\\ Q_1 & Q_0 & 0\\ 0 & 0 & 1\end{bmatrix}$

$$M_2 = \begin{bmatrix}6 & 2 & 0\\ 2 & 2 & 0\\ 0 & 0 & 1\end{bmatrix} \; with \; {M_2}^{-1} = \begin{bmatrix}\frac{1}{4} & -\frac{1}{4} & 0\\ -\frac{1}{4} & \frac{3}{4} & 0\\ 0 & 0 & 1\end{bmatrix}$$

Now $C = M_1 \times M_2 = \begin{bmatrix}-39 & -18 & 0\\ -39 & -17 & 0\\ -35 & -20 & -15\\ -35 & -20 & -4\\ -35 & -19 & 0\end{bmatrix} \times \begin{bmatrix}6 & 2 & 0\\ 2 & 2 & 0\\ 0 & 0 & 1\end{bmatrix}$

$$= \begin{bmatrix}-270 & -114 & 0\\ -268 & -112 & 0\\ -250 & -110 & -15\\ -250 & -110 & -4\\ -248 & -108 & 0\end{bmatrix}$$

Applying Vigenère Cipher with key

T	R	E	E
19	17	4	4

Offset rule with Key

x	-270	-114	0	-268	-112	0	-250	-110	-15	-250	-110	-4	-248	-108	0
vigenere	+ 19	+ 17	+ 4	+ 4	+ 19	+ 17	+ 4	+ 4	+ 19	+ 17	+ 4	+ 4	+ 19	+ 17	+ 4
	-251	-97	4	-264	-93	17	-246	-106	4	-233	-106	0	-229	-91	4
mod 26	9	7	4	22	11	17	14	24	4	1	24	0	5	13	4

Encrypted message is JHEWLROYEBYAFNE

Decryption: Message to be decrypted is

Message	J	H	E	W	L	R	O	Y	E	B	Y	A	F	N	E
Decimal Equivalent	9	7	4	22	11	17	14	24	4	1	24	0	5	13	4
Reverse vigenere cipher	- 19	- 17	- 4	- 4	- 19	- 17	- 4	- 4	- 19	- 17	- 4	- 4	- 19	- 17	- 4
	-10	-10	0	18	-8	0	10	20	-15	-16	20	-4	-14	-4	0
Mod 26	-270	-114	0	-268	-112	0	10	20	-15	-250	20	-4	-248	-4	0

Now $C = \begin{bmatrix}-270 & -114 & 0\\ -268 & -112 & 0\\ -250 & -110 & -15\\ -250 & -110 & -4\\ -248 & -108 & 0\end{bmatrix}$

And then $X = C \times {M_2}^{-1} = \begin{bmatrix}-270 & -114 & 0\\ -268 & -112 & 0\\ -250 & -110 & -15\\ -250 & -110 & -4\\ -248 & -108 & 0\end{bmatrix} \times \begin{bmatrix}\frac{1}{4} & -\frac{1}{4} & 0\\ -\frac{1}{4} & \frac{3}{4} & 0\\ 0 & 0 & 1\end{bmatrix}$

$$= \begin{bmatrix}-39 & -18 & 0\\ -39 & -17 & 0\\ -35 & -20 & -15\\ -35 & -20 & -4\\ -35 & -19 & 0\end{bmatrix}$$

In the final level of decryption, the optimal tree can be constructed with the private key shared.

7 Conclusion

The built-in cryptosystem, with public key cryptography as an enhancement, is more reliable than the system using symmetric key cryptography. In conclusion, the Multiphase Encryption Method emerges as a cutting-edge solution to the escalating demand for heightened data security. By harnessing the power of graph theory, mathematical matrices, and historical ciphers, this method introduces an innovative paradigm for encryption, effectively raising the bar against potential cyber threats. As technology continues to evolve, the pursuit of more secure encryption techniques remains a constant endeavour, and this research represents a significant step forward in fortifying data protection in the digital age.

REFERENCES

[1]."Cryptography: A very short introduction", Fred Piper and Sean Murthy.

[2]. "Introduction to Cryptography" J.Buchman, Springer-Verlag, 2001.

[3]. Neal Koblitz, "A Course in Number Theory and Cryptography".

[4] K.H.Rosen, "Elementary Number Theory and Its Applications," Third edition., AddsonWesly
[5] A. ChandraSekhar, D. Chaya Kumari, S. Ashok Kumar "Symmetric Key Cryptosystem for Multiple Encryptions",International Journal of Mathematics Trends and Technology (IJMTT). V29 (2):140-144 January 2016. ISSN:2231-5373.
[6] Gupta, Himanshu, and Vinod Kumar Sharma. "Multiphase encryption: A new concept in modern cryptography." *International Journal of Computer Theory and Engineering* 5.4 (2013): 638.
[7] Mishra, Rajalaxmi, Jibendu Kumar Mantri, and Sipali Pradhan. "New Multiphase Encryption Scheme for Better Security Enhancement." *IOT with Smart Systems*. Springer, Singapore, 2022. 599-606.
[8] Kaur, Harbir, Hirday Pal Singh Gill, and Dipti Sarmah. "Multiphase and Multiple Encryption." *2018 IEEE Punecon*. IEEE, 2018.
[9] Beliakov, Gleb, and Jozo Dujmović. "Extension of bivariate means to weighted means of several arguments by using binary trees." *Information sciences* 331 (2016): 137-147.
[10] Klein, Rolf, and Derick Wood. "On the path length of binary trees." *Journal of the ACM (JACM)* 36.2 (1989): 280-289.
[11] Hu, T. C., and K. C. Tan. "Path length of binary search trees." *SIAM Journal on Applied Mathematics* 22.2 (1972): 225-234.
[12] Crescenzi, Pierluigi, Giuseppe Di Battista, and Adolfo Piperno. "A note on optimal area algorithms for upward drawings of binary trees." *Computational Geometry* 2.4 (1992): 187-200.
[13] Koshy, Thomas. *Pell and Pell-Lucas numbers with applications*. Vol. 431. New York: Springer, 2014.
[14] Gökbas, Hasan, and H. Köse. "Some sum formulas for products of Pell and Pell-Lucas numbers." *Int. J. Adv. Appl. Math. and Mech* 4.4 (2017): 1-4.
[15] Fayeab, Bernadette, and Florian Lucab. "Pell and Pell-Lucas numbers with only one distinct digit." *Annales Mathematicae et Informaticae*. Vol. 45. 2015.
[16] Dasdemir, Ahmet. "On the Pell, Pell-Lucas and modified Pell numbers by matrix method." *Applied Mathematical Sciences* 5.64 (2011): 3173-3181.
[17] Nasution, Surya Darma, et al. "Data security using vigenere cipher and goldbach codes algorithm." *Int. J. Eng. Res. Technol* 6.1 (2017): 360-363.
[18] Soofi, Aized Amin, Irfan Riaz, and Umair Rasheed. "An enhanced vigenere cipher for data security." *Int. J. Sci. Technol. Res* 5.3 (2016): 141-145.
[19] Aliyu, Al-Amin Mohammed, and Abdulrahman Olaniyan. "Vigenere Cipher: Trends, Review and Possible Modifications." *International Journal of Computer Applications* 135.11 (2016): 46-50.
[20] Kester, Quist-Aphetsi. "A Hybrid Cryptosystem based on Vigenere cipher and Columnar Transposition cipher." *arXiv preprint arXiv:1307.7786* (2013).
[21] Gudela Ashok, S. Ashok Kumar, D. Chaya Kumari & Mathe Ramakrishna (2022) A type of public cryptosystem using polynomials and pell sequences, Journal of Discrete Mathematical Sciences andCryptography, 25:7, 19511963, DOI: 10.1080/09720529.2022.2133237
[22] "Super-Encryption Method using Affine Transform Via Trees" Beena Kittur, D. Chaya Kumari, Sneha G. Kulkarni, Manjula K M, International Journal of Mathematics Trends and Technology, Volume 68 Issue 6