Journal of Information Systems Engineering and Management
2025, 10(14s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cryptography Security of Digital Signals using Golden Matrix with Recurrence Relations

Esh Narayan[1], Dr. Abhishek Mishra[2], Sunil Kumar Singh[3]
[1]Research Scholar, Computer Science and Engineering, IFTM University, Moradabad 244102.UP INDIA
[2]Assistant Professor, Computer Science and Engineering, IFTM University, Moradabad 244102.UP INDIA
[3]Research Scholar, Electrical Engineering, IFTM University, Moradabad 244102 UP INDIA
E.Mail. Id.
EN, narayanesh1984@gmail.com
AM, abhimishra2@gmail.com
SKS, suneeli25@gmail.com

ARTICLE INFO

Received: 22 Nov 2024

Revised: 16 Jan 2025

Accepted: 30 Jan 2025

ABSTRACT

Modern cryptography is a field of study and practice that involves creating secure communication and data protection systems. Its primary goal is to ensure authenticity, integrity, and confidentiality of information in the presence of adversaries or potential attackers. Digital signatures are a crucial component of modern cryptography, providing validation, data privacy protection in digital communication. These are used to verify the authenticity of a digital message or document and ensure that no changes have been made to it since the signature was applied. . We can explore new methods for safeguarding digital signals using the Golden Matrix. The golden matrix, constructed using mathematical principles of the golden ratio, exhibits self-similarity and deterministic complexity, making it a robust foundation for encryption. Recurrence relations, such as those found in Fibonacci sequences, add an additional layer of security by introducing dynamic and pseudo-random transformations. We want to compare the time complexity in FP transform and Vigenere Cipher. Time complexity of the proposed algorithms is better than Vigenere Cipher also proposed algorithms have multilevel security so it's more secure and authenticate for networks. Furthermore, the method's efficiency makes it suitable for real-time digital signal encryption, such as video streaming, audio communication, and data transfer. Experimental results demonstrate the robustness, scalability, and computational efficiency of this technique, proving its viability for securing digital communication in modern networks.

Keywords: FP Transform, Time complexity, Vigenere Cipher, Recurrence, Encryption etc.

1. Introduction

Recurrence relations are mathematical equations that define a sequence based on its previous terms. Golden matrices could refer to matrices related to the golden ratio or other mathematical concepts [12]. While these mathematical concepts might find applications in various fields, including signal processing, their specific use in cryptography would depend on the development of new algorithms or protocols. Modern cryptography is a field of study and practice that involves creating secure communication and data protection systems. Its primary goal is to ensure authenticity, integrity, and confidentiality of information in the presence of adversaries or potential attackers. Digital signatures are a crucial component of modern cryptography, providing validation, data privacy protection in digital communication. These are used to verify the authenticity of a digital message or document and ensure that no changes have been made to it since the signature was applied [5]. They are used to verify the authenticity of a digital message or document and ensure that it has not been altered since the signature was applied. We can explore new methods for safeguarding digital signals using the Golden Matrix. In today's world, cryptography plays a crucial role; encryption and decryption depend on a piece of confidential information, typically referred to as a key. [1].

1.1. Fibonacci number

Fibonacci numbers are the numbers of the following integer sequence, called the Fibonacci sequence. The recurrence satisfied by the Fibonacci numbers is the arc type of a homogeneous linear recurrence relation with constant coefficients [1]. Defined as the recurrence relation are:

$\mathbf{F_{n+1} = F_n + F_{n-1}}$.

With the primary conditions: $F_1 = 1 \; and \; F_2 = 1$.

These integer numbers are called the Fibonacci sequence 1, 1, 2, 3, 5, 8........

$$F^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

$$F^1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (2)$$

1.2. Pell Number

The primary Pell numbers are $P_1 = 1, P_2 = 2$ and other terms of the sequence are obtained by means of the recurrence relation $\mathbf{P_{n+1} = 2P_n + P_{n-1}, n \geq 2}$

The recurrence relation of Pell Numbers is shown as:

$$P^n = \begin{cases} 0 & if\ n = 0 \\ 1 & if\ n = 1 \\ \mathbf{P_{n+1} = 2P_n + P_{n-1}} & if\ n \geq 2 \end{cases} \dots\dots\dots\dots\dots\dots (3)$$

1.3.Fibonacci - Pell Transform

The mapping FB: $T^2 \to T^2$ is Fibonacci - Pell (FP) Transformation. It can be defined as

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \mathbf{F}_i & \mathbf{F}_{i+1} \\ \mathbf{P}_i & \mathbf{P}_{i+1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\boldsymbol{modN}) .$$

Where $x, y \in \{0,1,2, \dots . N - 1\}$ in this transformation where

F_i is the i^{th} term of fibonacci series and P_i is the i^{th} Pell series

Denoting $\begin{pmatrix} \mathbf{F}_i & \mathbf{F}_{i+1} \\ \mathbf{P}_i & \mathbf{P}_{i+1} \end{pmatrix}$.These transformations continue in this way.

1.4.Affine transformation:

For enciphering we can use affine transformation $C = aP + b(mod)N$ where the pair (a, b) in the encrypting key and gcd (a, N) = 1.We can be used for deciphering $P = a^{-1}(y - b)mod26$

2. Proposed work

2.1.Encryption_algorithms:

Step 1: Let the plain text p be a square matrix of order, $\boldsymbol{n} > 0$. Let $\boldsymbol{A_i}$ be the choice of $\boldsymbol{i^{th}}$ permutation. Then Alice creates:

$Plain\ text: p = p_1, p_2, \dots \dots . . p_n.$

Step 2: A Computes $C = p \times (FP)$ and get first ciphertext.

Step 3: Then Alice performs encryption with C to affine transformation is

$E(x) = (ax + b)mod26$, GCD (a, N) = 1 and a and b are secret key.

Step 4: Alice sends super encrypted massage to Bob.

2.2. Decryption_algorithms

Step 1: Super encrypted can be obtained by Massage Bob

Step 2: Bob decrypts using super encrypted massage by $E^{-1}(y) = a^{-1}(y - b)mod26 = (p^1)$

Step 3: Bob compute$A = p^1 \times (FP)^{-1}$. To get the original massage

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example-

Case -1: For$i = 1$, Put them in Fibonacci - Pell $(FP) = \begin{pmatrix} F_1 & F_2 \\ P_1 & P_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$................ (4)

A. Encryption algorithms:

Step 1: Let the plane text

$p = \begin{pmatrix} E & S \\ H & U \end{pmatrix} = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix}$........................... (5)

Step 2: Then we find the value

$C = p \times (FP)$ .... (6)

$C = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 22 & 40 \\ 27 & 47 \end{pmatrix}$ .... (7)

Step 3: Now we can be used affine transformation $E(x) = (ax + b)mod26$ for $a = 5, b = 25$

x	22	40	27	47
$x mod\ 26$	22	14	1	21
$5x + 25$	135	95	30	130
(5x + 25)mod 26	5	17	4	0
Massage	F	R	E	A

Table 1- find first Encrypted massage in first phase by proposed algorithms

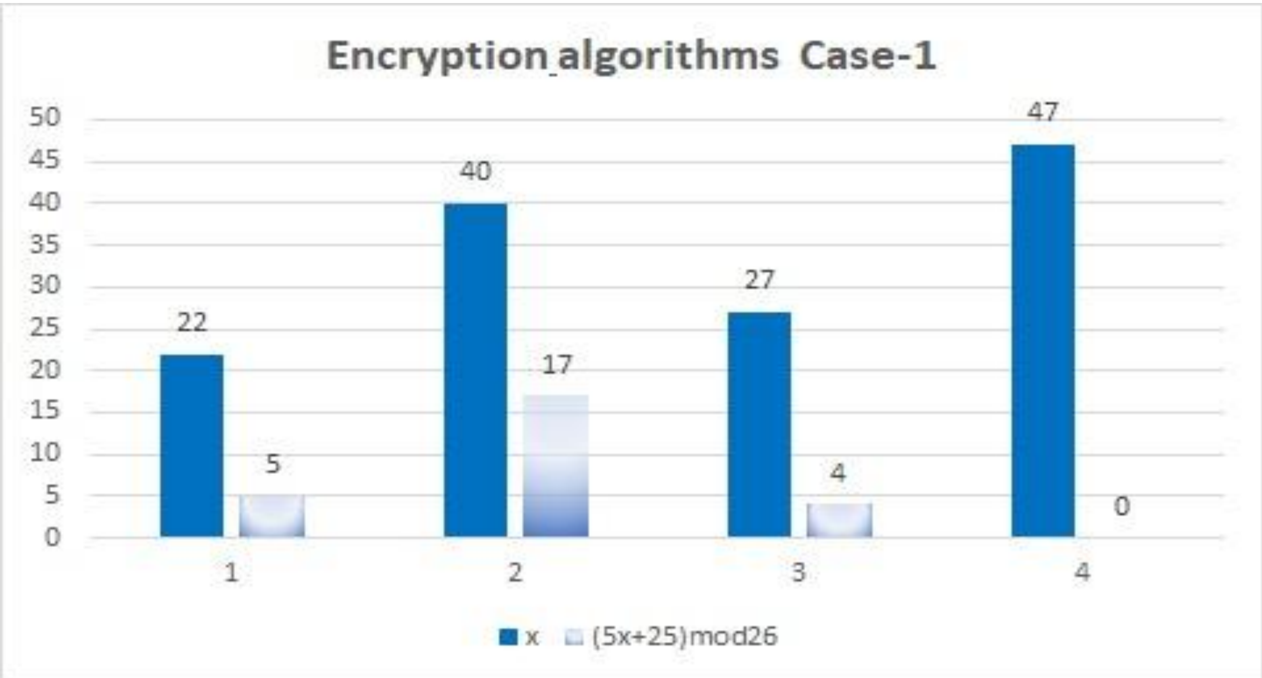

Figure -1:- Encrypted data case 1

Step 4: FREA is Encrypted message.

B. Decryption algorithms:

Step 1: First Decrypted message is FREA

Step 2: Compute the inverse affine transform $E^{-1}(y) = a^{-1}(y-b)mod26$

Massage	F	R	E	A
y	5	17	4	0
$y-25$	-20	-8	-21	-25
$21(y-25)$	-420	-168	-441	-525
(y − 25)mod26	22	14	1	21
First decrypted text	W	O	B	V

Table 2- find first decrypted massage in first phase by proposed algorithms

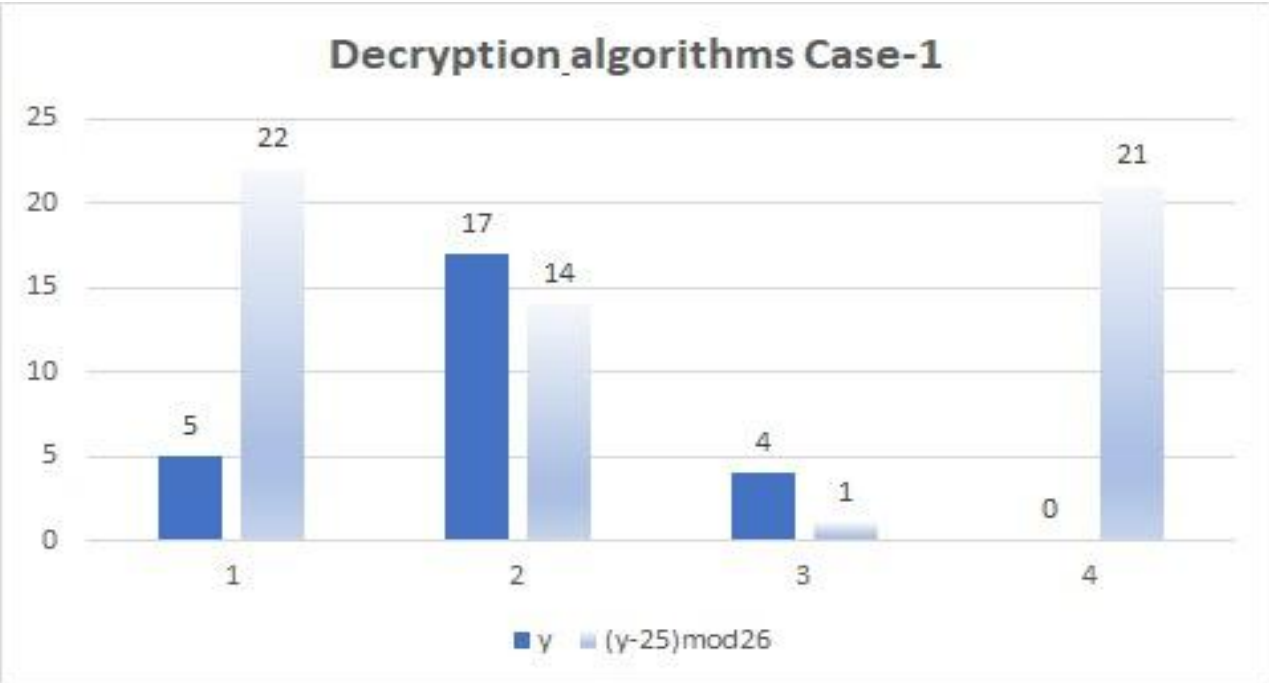

Figure -2:- Decrypted data case 1

THEN $p^1 = \begin{pmatrix} W & O \\ B & V \end{pmatrix} = \begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix}$ .... (8

Step 3: Bob compute $p = p^1 \times (FP)^{-1}$ *now*

$\begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 30 & -8 \\ -19 & 20 \end{pmatrix}$............ (9)

Value	30	-8	-19	20
$mod26$	4	18	7	20
Second Decrypted Text	E	S	H	U

Table 3- find final massage in first phase by proposed algorithms

$p = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} = \begin{pmatrix} E & S \\ H & U \end{pmatrix}$ .... (10)

This is a message exchanged between Alice and Bob.

Case -2: For$i = 2$, Put them in Fibonacci - Pell $(FP) = \begin{pmatrix} F_2 & F_3 \\ P_2 & P_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$................ (11)

A. Encryption_algorithms:

Step 1: Let the plane text

$p = \begin{pmatrix} E & S \\ H & U \end{pmatrix} = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix}$........................... (12)

Step 2: Then we find the value

$C = p \times (FP)$ .... (13)

$C = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 40 & 98 \\ 47 & 114 \end{pmatrix}$ .... (14)

Step 3: Now we can be used affine transformation $E(x) = (ax + b)mod26$ for $a = 5, b = 25$

x	40	98	47	114
$xmod\ 26$	14	20	21	10
$5x + 25$	95	125	130	75
$(5x + 25)$mod 26	17	21	0	23
Massage	R	V	A	X

Table 4- find first Encrypted massage in second phase by proposed algorithms

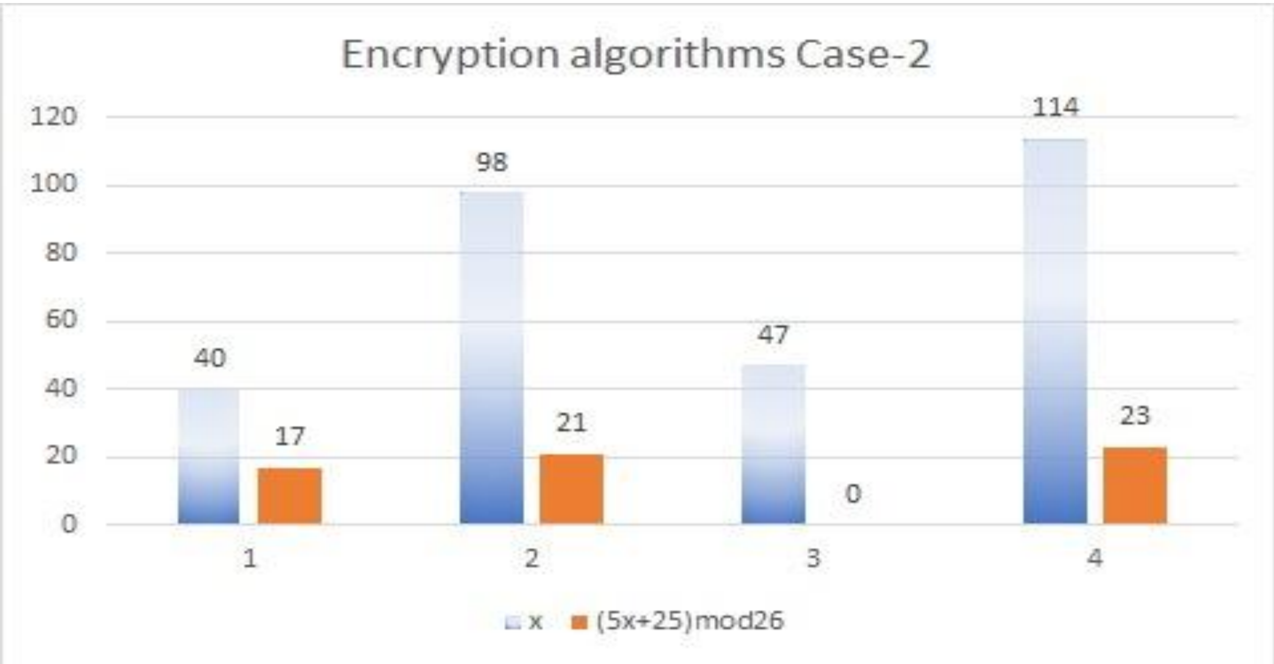

Figure -3:- Encrypted data case 2

Step 4: RVAX is Encrypted message.

B. Decryption_algorithms

Step 1: First Decrypted message is FREA.

Step 2: Compute the inverse affine transform $E^{-1}(y) = a^{-1}(y - b)mod26$

Massage	R	V	A	X
y	17	21	0	23
$y-25$	-8	-4	-25	-2
$21(y-25)$	-168	-84	-525	-42
$(y-25)\text{mod}26$	14	20	21	10
First decrypted text	O	U	V	K

Table 5- find first decrypted massage in second phase by proposed algorithms

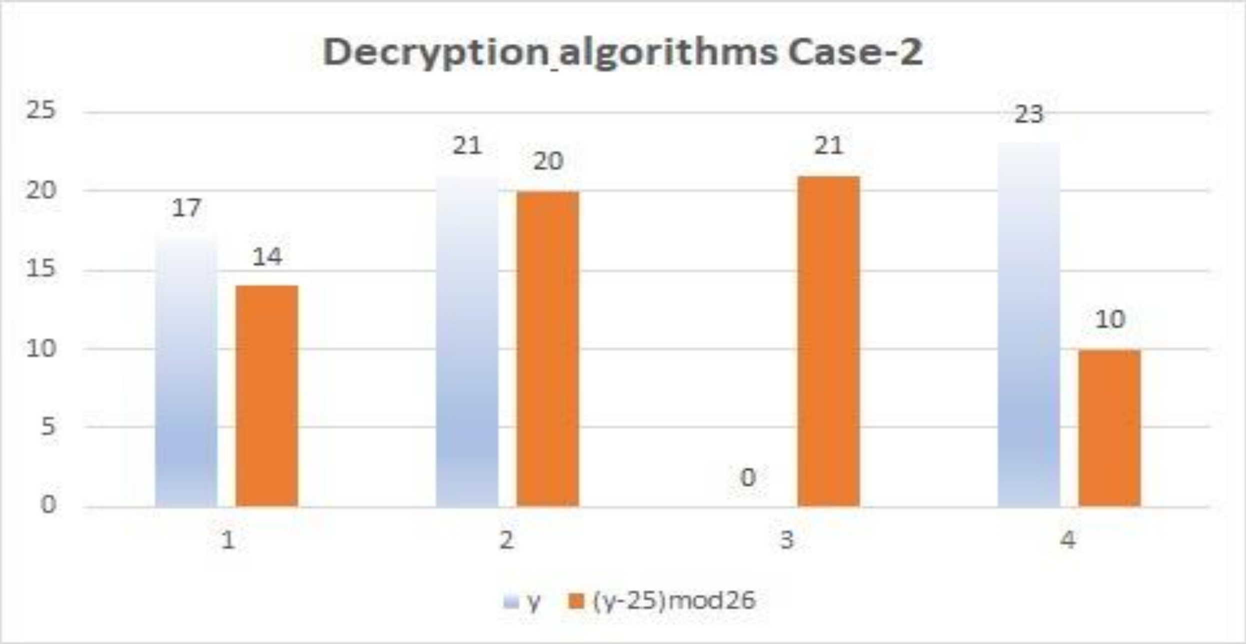

Figure -4:- Decrypted data case 2

THEN $p^1 = \begin{pmatrix} O & U \\ V & K \end{pmatrix} = \begin{pmatrix} 14 & 20 \\ 21 & 10 \end{pmatrix}$ .... (15)

Step 3: Bob compute $p = p^1 \times (FP)^{-1} \quad now$

$\begin{pmatrix} 14 & 20 \\ 21 & 10 \end{pmatrix} \times \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 30 & -8 \\ 85 & -32 \end{pmatrix}$........... (16)

Value	30	-8	85	-32
$mod26$	4	18	7	20
Second Decrypted Text	E	S	H	U

Table 6- find final massage in second phase by proposed algorithms

$P = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} = \begin{pmatrix} E & S \\ H & U \end{pmatrix}$ .... (17)

This is a message exchanged between Alice and Bob.

3. Vigenere Cipher

The Vigenere cipher encrypts alphabetic text through a basic poly alphabetic substitution. A poly alphabetic cipher employs multiple substitution alphabets, making it more resistant to frequency analysis compared to a mono alphabetic cipher, where each letter is replaced by a consistent counterpart. Here's how the Vigenere cipher works:

Key: The key is a word or phrase that is repeated to match the length of the plaintext.

Encryption In the Vigenere cipher, each letter in the plaintext is shifted based on its corresponding letter in the key, with the key letter determining the shift amount. A Vigenere square, a tabular arrangement of the alphabet, is commonly used to find these shift values.

Decryption: To decrypt, the process is reversed. Each letter in the cipher text is shifted backward based on the corresponding letter in the key.

Example

Case -1: For $i = 1$, Put them in Fibonacci - Pell (FP) = $\begin{pmatrix} F_1 & F_2 \\ P_1 & P_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$................ (18)

Encryption algorithms:

Step 1: Let the plane text

$p = \begin{pmatrix} E & S \\ H & U \end{pmatrix} = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix}$.............................. (19)

Step 2: Then we find the value

C = p × (FP) .. .. (20)

$C = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 22 & 40 \\ 27 & 47 \end{pmatrix}$ .... (21)

Step 3: Now we can be used offset Rule using key – PASS

P	A	S	S
15	0	18	18

x	22	40	27	47
x+ key	22+15	40+0	18	18
	37	40	45	65
mod 26	11	14	19	13
Massage	L	O	T	N

Table 7- find first Encrypted massage in first phase by Vigenere cipher

Step 4: LOTN is First Decrypted message.

Decryption algorithms:

Step 1: LOTN is First Decrypted message.

Step 2: Compute the inverse

Massage	L	O	T	N
y	11	14	19	13
$y - key$	11-15	14-0	19-18	13-18
	-4	14	1	-5
mod26	22	14	1	21
First decrypted text	W	O	B	V

Table 8- find first Decrypted massage in first phase by Vigenere cipher

THEN $A_1 = \begin{pmatrix} W & O \\ B & V \end{pmatrix} = \begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix}$ .... (22)

Step 3: Bob compute $p = p^1 \times (FP)^{-1} \quad now$

$\begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 30 & -8 \\ -19 & 20 \end{pmatrix}$............. (23)

Value	30	-8	-19	20
$mod26$	4	18	7	20
Second Decrypted Text	E	S	H	U

Table 9- find final massage in first phase by Vigenere cipher

$P = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} = \begin{pmatrix} E & S \\ H & U \end{pmatrix}$ .... (24)

This is a message exchanged between Alice and Bob.

Case -2: For $i = 2$, Put them in Fibonacci - Pell $(FP) = \begin{pmatrix} F_2 & F_3 \\ P_2 & P_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$................ (25)

Encryption_algorithms:

Step 1: Let the plane text

$A = \begin{pmatrix} E & S \\ H & U \end{pmatrix} = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix}$........................... (26)

Step 2: Then we find the value

$C = p \times (FP)$

C= $\begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 40 & 98 \\ 47 & 114 \end{pmatrix}$ .... (27)

Step 3: Now we can be used offset Rule using key – PASS

x	40	98	47	114
$x + key$	40+15	98+0	47+18	114+18
	55	98	65	132
mod 26	3	20	13	2
Massage	D	U	N	C

Table 10- find first Encrypted massage in second phase by Vigenere cipher

Step 4: DUNC is Encrypted message.

Decryption_algorithms:

Step 1: DUNC is First Decrypted message.

Step 2: Compute the inverse affine transform

Massage	D	U	N	C
y	3	20	13	2
$y - key$	3-15	20-0	13-18	2-18
	-12	20	-5	-16
mod26	14	20	21	10
First decrypted text	O	U	V	K

Table 11- find first Decrypted massage in second phase by Vigenere cipher

THEN $A_1 = \begin{pmatrix} O & U \\ V & K \end{pmatrix} = \begin{pmatrix} 14 & 20 \\ 21 & 10 \end{pmatrix}$ .... (28)

Step 3: Bob compute $p = p^1 \times (FP)^{-1} \quad now$

$\begin{pmatrix} 14 & 20 \\ 21 & 10 \end{pmatrix} \times \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 30 & -8 \\ 85 & -32 \end{pmatrix}$.......... (29)

Value	30	-8	85	-32
$mod26$	4	18	7	20
Second Decrypted Text	E	S	H	U

Table 12- find final massage in second phase by Vigenere cipher

$$P = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} = \begin{pmatrix} E & S \\ H & U \end{pmatrix} \quad \text{.....................} (30)$$

This is a message exchanged between Alice and Bob.

4. Discssion and Analisis

In this chapter we want to compare the time complexity in proposed algorithms using FP transform and Vigenere Cipher. Time complexity of the proposed algorithms is better than Vigenere Cipher also proposed algorithms have multilevel security so it's more secure and authenticate for networks.

4.1.Time complexity: We see the results of time complexity in both algorithms in encryption and decryption.

A. Encryption and decryption in Vigenere Cipher:

Start Encryption using Vigenere Cipher at: 12/06/2024 08:35:28.608 PM

End Encryption using Vigenere Cipher at: 12/06/2024 08:35:28.616 PM

Start Decryption using Vigenere Cipher at: 12/06/2024 08:35:28.616 PM

End Decryption using Vigenere Cipher at: 12/06/2024 08:35:28.632 PM

B. Encryption and decryption in Proposed Process:

Start Encryption using Proposed Process at: 12/06/2024 08:35:40.753 PM

End Encryption using Proposed Process at: 12/06/2024 08:35:40.753 PM

Start Decryption using Proposed Process at: 12/06/2024 08:35:40.753 PM

End Decryption using Proposed Process at: 12/06/2024 08:35:40.769 PM

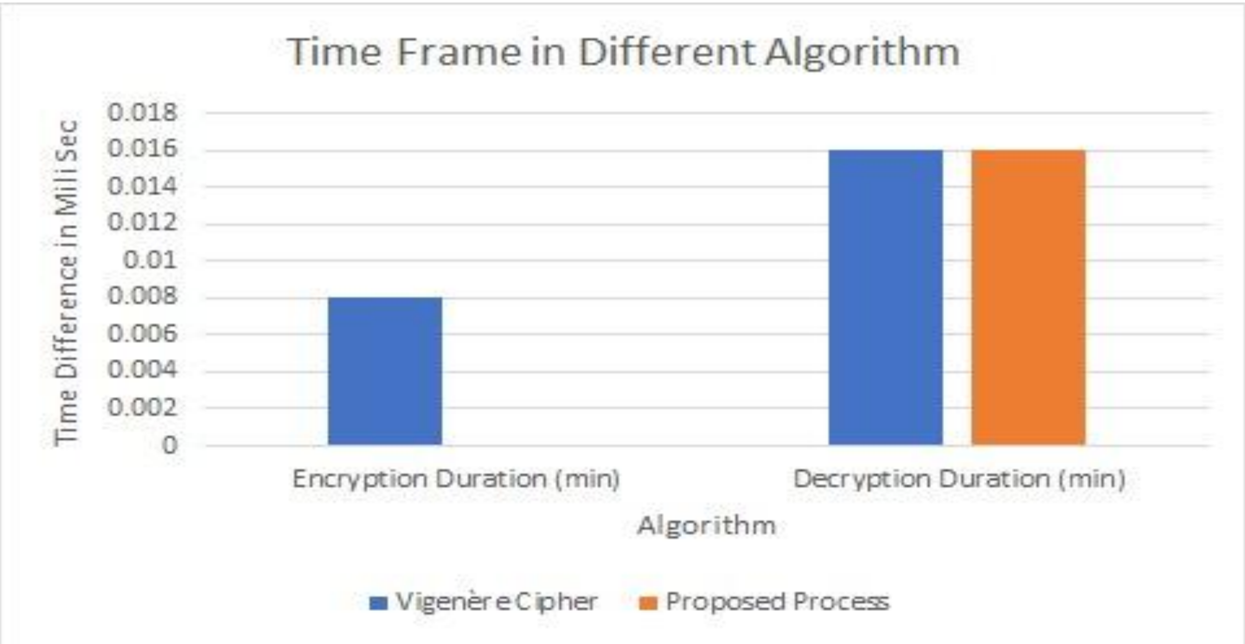

Figure -5 time frame graphs

We see the encryption time of Vigenere cipher is (.008) is high to comparison proposed algorithms is (0) And decryption time is same.

4.2. Multi level security:

In proposed algorithms have multilevel security, FP transform for encryption and affine transform for super encryption so its level of security is high? Proposed algorithms are more secure and reliable for network security.

5. Conclusion and Future scope

Data security plays an important role in current times. For security reasons, many algorithms have been implemented in modern cryptography. Proposed algorithms have multilevel security, FP transform for encryption and affine transform for super encryption and gave better results than other algorithms. This approach offers a secure and non-linear encryption mechanism. The golden matrix introduces self-similarity and pseudo-random transformations, while recurrence relations add dynamic adaptability, enhancing resistance to cryptanalysis and brute-force attacks. We compare the time complexity in proposed algorithms using F-P transform and Vigenere cipher then we found proposed algorithms have a low time complexity. Proposed algorithms are more secure and reliable for network security because it's have multilayer security. In future it's used for data security and high integrity.

Reference

[1] Esh Narayan, Abhishek Mishra, Sunil Kr. Singh **"**Cryptography Protection of Digital Signals using Fibonacci - Pell Transformation via Golden Matrix" IJEAT at Volume-10 Issue-2, December 2020. DOI:10.35940/ijeat.B2069.1210220

[2] K.R. Sudha, A. Chandra Sekhar, Prasad Reddy, Cryptography Protection of Digital Signals using Some Recurrence Relations. IJCSNS international journal of computer science and network security. VOL-7 No-5 in May 2007. http://paper.ijcsns.org/07_book/200705/20070530.pdf

[3] Prasanta Kumar Ray and PROF. G. K. Panda, "Balancing and Cobalancing numbers" in 2014.http://ethesis.nitrkl.ac.in/2750/1/Ph.D._Thesis_of_P.K._Ray..pdf

[4] Sujata Swain, Chidananda Pratihary and Prasanta Kumar Ray "Balancing and Lucas-Balancing Numbers and Their Application to Cryptography" Computer Engineering and Applications Vol. 5, No. 1, February 2016. DOI:10.18495/comengapp.v5i1.46

[5] Fatemeh Mohebalizad ehgashti, Professor F.M. Defersha Balancing, Sequencing and Determining the Number and Length of Workstations in a Mixed in Model Assembly Line April 2016. http://hdl.handle.net/10214/9662

[6] A.P. Stakhov "Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas functions, and the improved method of the golden cryptography" in 2006.
DOI: 10.4236/am.2014.53039

[7] Feras Bani-Ahmad, Mohd Taib Shatnawi, Nedal Tahat, Safaa Shatnawi "A new kind of digital signature scheme using golden matrices based on factoring problem" International Journal of Pure and Applied Mathematics Volume 107 No. 1 2016, 49-57.
Doi: 10.12732/ijpam.v107i1.5

[8] M. Tahghighi, S. Turaev, A. Jaafar, R. Mahmod and M. Md. Said "On the Security of Golden Cryptosystems" Int. J. Contemp. Math. Sciences, Vol. 7, 2012, no. 7, 327 – 335
https://m-hikari.com/ijcms/ijcms-2012/5-8-2012/turaevIJCMS5-8-2012.pdf

[9] Chandra Sekhar, Ch. Pragathi, D. Chaya Kumari and Ashok Kumar "Multiple Encryptions of Fibonacci Lucas transformations" IOSR Journal of Mathematics (IOSR-JM) e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 12, Issue 2 Ver. II (Mar. - Apr. 2016). DOI: 10.9790/5728-1202026672

[10] Mohammad Tahghighi Sharabyan "On the Security of Golden Cryptosystems" Int. J. Contemp. Math Sciences, Vol. 7, 2012.https://doi.org/10.18280/ts.390501

[11] Ernatuti, Ravi A Salim, Sulistyo "The application of "elc number to golden cryptography" The 5th International Conference on Information & Communication Technology and Systems IN 2011

[12] Ray, Prasanta Kumar, Panda, G K Balancing and Cobalancing Numbers. Ph.D. thesis on 29 Jun 2011. DOI:10.1155/IJMMS.2005.1189

[13] Tony D. Noe, Jonathan Vos Post "Primes in Fibonacci n-step and Lucas n-step Sequences" Journal of Integer Sequences, Vol. 8 (2005).
https://cs.uwaterloo.ca/journals/JIS/VOL8/Noe/noe5.pdf

[14] Mohammad Tahghighi, Azmi Jafaar, Ramlan Mahmod "Generalization of Golden Cryptography based on k-Fibonacci Numbers" International Conference on Intelligent Network and Computing (ICINC 2010).
https://repository.dinus.ac.id/docs/jurin/15282.pdf

[15] Thokchom Chhatrajit Singh "Lucas Numbers and Cryptography" National institute of technology rourkela, orissa-769008 in 2012.
http://ethesis.nitrkl.ac.in/3365/2/main.pdf

[16] Angel Martin Del Ray and Gerardo Rodriguez Sanchez "On the security of Golden cryptography" international journal of network security. VOL7 No.3 Nov. 2007.
http://ijns.jalaxy.com.tw/contents/ijns-v7-n3/ijns-2008-v7-n3-p448-450.pdf

[17] Prasanta Kumar Ray and Juli Sahu "Generating functions for certain balancing and Lucas-Balancing numbers" Palestine Journal of Mathematics Vol. 5(2) (2016), 122–129.
https://pjm.ppu.edu/sites/default/files/papers/PJM_Sep_2016_15.pdf

[18] Bijan Kumar Patel, Shanta Kumari Sunanda, and Prasanta Kumar Ray "Period of balancing numbers modulo product of consecutive Lucas-Balancing numbers" mathematica, 60 (83), No 2, 2018.
https://math.ubbcluj.ro/~mathjour/fulltext/2016/ray-patel.pdf

[19] Fatima Amounas, El Hassan El Kinani, Moha Hajar "Confidential Algorithm for Golden Cryptography Using Haar Wavelet" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 12, No. 8, August 2014. https://doi.org/10.48550/arXiv.1501.03617

[20] Fatima Amounas, El Hassan El Kinani, Moha Hajar "A Matrix Approach for Information Security Based ECC using Mealy Machine and Fibonacci Q-matrix" International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013
https://ijeit.com/Vol%203/Issue%201/IJEIT1412201307_95.pdf

[21] Sergiy Koshkin, Taylor Styers "From golden to unimodular cryptography" Chaos, Solitons, and Fractals 105 (2017) 208–214. https://doi.org/10.48550/arXiv.1904.00732

[22] Krishna Gandhi, A. Chandra Sekhar, S. Sri Lakshmi "Encryptions of Data Streams using Pauli Spin ½ Matrices and Finite State Machine" International Journal of Computer Applications (0975 – 8887) Volume 37– No.2, January 2012.
https://research.ijcaonline.org/volume37/number2/pxc3876497.pdf

[23] Prasanta Kumar Ray, Gopal Krishna Dila, and Bijan Kumar Patel "Application of Some Recurrence Relations to Cryptography using Finite State Machine" International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 2, Issue 4 (2014) ISSN 2320–4028.https://journalsweb.org/siteadmin/upload/P1214019%20New.pdf

[24] Bijan Kumar Patel, Nurettin Irmak And Prasanta Kumar Ray "Incomplete Balancing And Lucas - Balancing Numbers" Math Reports 20(70), 1 (2018), 59-72
http://imar.ro/journals/Mathematical_Reports/Pdfs/2018/1/6.pdf

[25] Ravi Kumar, A. Chandra Sekhar, G. Appala Naidu "A Novel ElGamal Encryption Scheme of Elliptic Curve Cryptography" International Journal of Computer Trends and Technology (IJCTT) in 20/02/ 2015.DOI:10.14445/22312803/IJCTT-V20P114

[26] Licinius Dimitri Sa de Alcantar Towards a simple and secure method for binary cryptography via linear algebra Revista Brasileira de Computacao Aplicada (ISSN 2176-6649), Passo Fundo, v. 9, n. 3, p. 44-55, out. 2017
DOI:10.5335/rbca.v9i3.6556

[27] Ravi Kumar Davala and G. K. Panda "On sum and ratio formulas for balancing-like sequences" Print ISSN 1310–5132, Vol. 22, 2016, No. 3.
https://www.researchgate.net/publication/271201375

[28] K. C. Gowda and T. R. Ravi, "Clustering of symbolic objects using gravitational approach," IEEE Trans. on Systems Man Cybernetic, vol. 29, no. 6, pp. 888–894, 1999.
DOI: 10.1109/3477.809041

[29] S. Guru, B. B. Kiranagi and P. Nagabhushan, “Multivalued type proximity measure and concept of mutual similarity value useful for clustering symbolic patterns,” Pattern Recognition Letter, vol. 25, pp. 1203–1213, 2004.
https://doi.org/10.1016/j.patrec.2004.03.016