International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-2, December 2020

Cryptography Protection of Digital Signals using Fibonacci - Pell Transformation via Golden Matrix

Esh Narayan, Abhishek Mishra, Sunil Kr. Singh

Abstract: ***At this time the security of communication can be the important role of electronic communication. In this paper we can discuss the new transform for the protection of digital signals using with golden matrix. Fibonacci - Pell (FP) Transform can be find sufficient results to secure the signals and the aims of this paper to describe the security of signals using new type of recurrence formula. The recurrence relation can be find sufficient results to secure the signals. Multiple encryptions are used in this algorithm. Fibonacci - Pell (FP) Transform used for encryption and affine cipher can be used for super encryption. It ensures that to secure the data from attackers in this cryptographic method is fast and simple.***

Keywords: Golden cryptography (GC), Golden Matrix (GM), Fibonacci – Pell (FP) Transform, Recurrence Relation (RR), Learning Algorithm Improves (LAI)

I. INTRODUCTION

Overview of different methods and techniques used in signal protection in golden cryptography, Sudha K.R., A.Chandra Sekha, Prasad Reddy in 2007 says that the Communications security is very importance in electronic communications. Swain Sujata, Pratihary Chidananda and Ray Prasanta Kumar (2016) proposed that the method is well known that, recursive relation for the sequence $a_0, a_1, a_2, a_3, a_4, \ldots\ldots\ldots a_n$, are an equation that relates to certain of its preceding terms $a_0, a_1, a_2, a_3, a_4, \ldots\ldots\ldots a_{n-1}$, Initial conditions for the sequence $a_0, a_1, a_2, a_3, a_4, \ldots\ldots\ldots$ are explicitly given values for a finite number of the terms of the sequence.

GOLDEN MATRIX

If x is a real number then the mathematical form of golden matrices is defined as:

$$\boldsymbol{Q^{2x}} = \begin{pmatrix} \boldsymbol{cFs(2x+1)} & \boldsymbol{sFs(2x)} \\ \boldsymbol{sFs(2x)} & \boldsymbol{cFs(2x-1)} \end{pmatrix} \ldots\ldots\ldots\ldots (1)$$

$$\boldsymbol{Q^{2x+1}} = \begin{pmatrix} \boldsymbol{cFs(2x+2)} & \boldsymbol{sFs(2x+1)} \\ \boldsymbol{sFs(2x+1)} & \boldsymbol{cFs(2x)} \end{pmatrix} \ldots\ldots\ldots (2)$$

Where

$$\boldsymbol{sFs(x)} = \frac{T^x - T^{-x}}{\sqrt{5}}, \boldsymbol{cFs(x)} = \frac{T^x + T^{-x}}{\sqrt{5}} \ldots\ldots\ldots\ldots (3)$$

The equations 1and 2 are called golden matrices

These recurrence relations are useful in some counting problems such as Fibonacci numbers, Balancing numbers, Lucas- balancing numbers, Lucas numbers, etc.

Revised Manuscript Received on December 25, 2020.
* Correspondence Author
Esh Narayan*, Research Scholar,Computer Science and Engineering, IFTM University, Moradabad
Dr. Abhishek Mishra, Associate Professor, Computer Science and Engineering, IFTM University, Moradabad
Sunil Kr. Singh, Research Scholar, Electrical Engineering, IFTM University, Moradabad

We can be used recurrence relations for both equilibrium and Lucas – balancing numbers and investigates all application to cryptography.

LUCAS NUMBER

This is the recurrence formula of Lucas numbers $L_K$then defined the equation:

$$\mathbf{L_{K+1} = L_K + L_{K-1}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \mathbf{(4)}$$

With the initial condition $L_0 = 2, L_1 = 1$

$$L^n = \begin{pmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

$$L^{-n} = \frac{(-1)^n}{4} \begin{pmatrix} L_{n-1} & -L_n \\ -L_n & L_{n+1} \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots (6)$$

Where n= 1, 2, 3……

$$L^1 = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (7)$$

These are the (2× 2) matrix

LUCAS BALANCING NUMBER

This is the recurrence formula of Lucas-balancing numbers $\mathbf{C_n}$ then$\boldsymbol{C_n^2 = 8B_n^2 + 1}$

$$\mathbf{C_{n+1} = 6C_n - C_{n-1} n \geq 2} \quad \ldots\ldots\ldots\ldots\ldots\ldots \mathbf{(8)}$$

The initial condition $C_1 = 3, C_2 = 17$

$$C^n = \begin{pmatrix} C_{n-1} & -C_n \\ C_n & -C_{n-1} \end{pmatrix} \quad \ldots\ldots\ldots\ldots\ldots (9)$$

BALANCINGNUMBER

This is the recurrence formula of balancing number $\mathbf{B_n}$ **then**$\mathbf{B_{n+1} = 6B_n - B_{n-1}}$. Where B_n is a balencing number with Initial Condition?

$$B^n = \begin{pmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (10)$$

Then

$$B^1 = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (11)$$

But extended balancing number is

$$B^n = \begin{pmatrix} -B_{n-1} & -B_n \\ B_n & -B_{n+1} \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (12)$$

II. LITERATURE REVIEW

This literature review is carried out on the relevant topics of message exchanging problems using different forms of matrices. Various types of matrices like golden matrices, sparse matrices, etc. are considered in the survey. In this survey includes related topics like cryptography and the maximum recurrence relation.Mei-Chu Chang in 2013 find a new algorithm in cryptography is the product of a matrix. Let A,

B be invertible $n \times n$ matrices over the finite field F_q with irreducible characteristic polynomials.

For $k \epsilon Z^+$, it's denoted by $\boldsymbol{M_k(A,B) \coloneqq \{f(A)g(B): f,g \epsilon F_q[x], with \deg f, deg = k\}}$ **Assu** $\boldsymbol{\geq 2n}$ **, we prove that** $\boldsymbol{|M_k(A,B)| > 4^{-k} q^{\min(n,2k-1)}}$ Moreover, let $d = \dim \ker (AB - BA)$, then we prove that

$$|M_k(A,B)| > \frac{1}{(16\binom{n}{d})(2(n-d))^{\frac{n-d}{2}}} \; q^{\min(n,2k-1)}$$

Kalman Liptai, Florian Luca, Akos Pinter and Laszlo Szalay in 2009 proposed an algorithm in Generalized balancing numbers. The positive integer x is a (k,l)-balancing number for $y(x \leq y-2)$ if

$\mathbf{1^k + 2^k + \ldots + (1-x)^k = (x+1)^l + \cdots + (y-1)^l}$ For fixed positive integers $k$and$l$.Ray Prashant Kumar Ray and Prof. GK Panda in 2014 found that a different approach to the theory of equilibrium numbers is possible using a Pell equation that can be derived from the definition of equilibrium numbers. Each balancing number corresponds to a balancer. Likewise, each co-balancing number corresponds to a co-balancer and interestingly, each co-balancer is an equilibrium number. The Lucas-balancing and Lucas-co balancing numbers obtained respectively as functions of balancing and co-balancing numbers are useful in the computation of balancing and co-balancing numbers of higher order. A.P. Stakhov in 2014 considers the Gazelle formulas, which are a broad generalization of the Binet and Pell formulas, and a new class of Golden hyperbolic functions, a broad generalization of the symmetric hyperbolic Fibonacci and Lucas functions in 2005. In addition, we consider a new class of Golden matrices a broader generalization of Golden matrices (Stakhov, 2006). Ernatuti, Ravi a Salim, Sulistyo in 2010 has proposed the algorithms for the problem of protecting digital signals from hackers are usually solved with the application of cryptographic methods. "Golden" matrices can be used to create a new type of cryptography called Golden Cryptography. The method is very fast and simple for technical perception and can be used for cryptographic protection of digital signals. The literature demonstrated cryptography to be based on the Golden Matrices and iterative relationships of Fibonacci and Lucas numbers. More recently, in 2007, a sequence of new numbers called ELC was investigated. It was defined by the iterative formula of the number of extended Lucas cube vertices. We have found that a cryptographic algorithm is proposed and implemented based on the iteration relation of the ELC number. The performance of the algorithm is analyzed. This ensures the cryptographic security of digital signals used in telecommunications, and is quicker and simpler to realize. Monty Kester in 2010 has found the discovery of Leonard of Pisa, known as Fibonacci, is a revolutionary contribution to the mathematical world. His most famous work is the Fibonacci sequence, in which each new number is the sum of the preceding two numbers. When various operations and manipulations are performed on this sequence of numbers, beautiful and incredible patterns begin to emerge.Mohammad Tahghighi, Azmi Jafaar, RamlanMahmod (2010), Mohamad Rushdan Md. has proposed a new kind of cryptosystem using K-Fibonacci number. The golden cryptosystem was introduced to be insecure against the chosen-plaintext attack. We will show that this new cryptosystem, which is a modification of the golden cryptosystem, is secure against chosen-plaintext attacks. From the results in the preceding section, we can conclude that this new proposed generalized cryptosystem based on k-Fibonacci numbers is more secure than the original golden cryptography against chosen-plaintext attacks.

Angel Martin Del Rey and Gerardo Rodriguez Sanchez in 2008 have been provided the security of golden cryptography, which has recently been proposed, has been tackled. In particular, it has been shown that the security of such a crypto currency is trivially compromised because it does not pass one of the original crypto currency attacks: the Chosen-Plain attack.Prasanta Kumar Ray and JuliSahu in 2015 find new cryptography approaches the generating function for any sequence. This function is used to solve both homogenous and non-homogenous recurrence relations. We find generating function of certain balancing and Lucas-balancing numbers in this study, these functions are helpful in the protection of digital signals. Bijan Kumar Patel, Shanta Kumari Sunanda, and Prasanta Kumar Ray in 2010 have proposed a new thing in a period of the balancing numbers modulo, denoted by, is the least positive integer such that (mod m), where denotes the balancing number. We have found the periods of the balancing numbers modulo a product of consecutive Lucas-balancing numbers.Fatima Amounas, El Hassan El Kinani, Moha Hajar in 2013 has proposed a new algorithm in cryptography to the science of transmission and reception of secret messages. Nowadays the information security is essential in many operations in our everyday life. Many numbers of ciphersGeneration and decryption algorithms exist and are being evolved due to the increasing demand of users and e-commerce services. Message encryption has become very essential to avoid the threat against possible attacks by hackers during the transmission process of the message. We have found a new approach for secure information transmission over communication channels based on an elliptic curve using the mealy machine and Fibonacci Q-matrix. The proposed approach will not only enhance the security of information but also saves computation time and reduces power requirements that will find it' suitability for future handheld devices and online transaction processing. Licinius Dimitri Sa de Alcantara(2017) has been proposed a simple and secure binary matrix encryption (BME) method is proposed and formalized on a linear algebra basis. The developed cryptography scheme does not require the idealization of a set of complex procedures or the generation of parallel bit stream for encryption of data, but it only needs to capture binary data sequences from the unprotected digital data, which are transformed into encrypted binary sequences by a cipher matrix. This method can be performed on a physical or application layer level and can be easily applied to any digital storage and telecommunication system.

It also has the advantage that the encrypted data length is not increased, which avoids additional burden for data storage and transmission.
To validate the presented methodology, a GNU Octave program code was written to encrypt and decrypt data files. We prove some effective and ineffective balancing statements for the remaining numbers, using some Baker-type Diophantine results and the Billu – Tichy theorem, respectively. M. MohdHafizuddin, N.K Ahmad Nazif, Y. MohdNeedza and D. AzilaNadiah in 2012 have been proposed a Study on Line Balancing in Assembly Line at Automotive Component Manufacturer. Assembly line need to be designed properly base on the types of product, workloads required, numbers of daily production as well as other elements.

Table: The Comparison between different signal protection Techniques:

Sr. No.	Author Name	Year	Methodology Used	Highlights
1	K.R. Sudha et al.[1]	2007	Recurrence relations in the continuous domain	Improving cryptographic security in digital signals and is also faster and simpler for realization
2	Prof. G.K. Pandaet al. [2]	2009	Theory of balancing number	Theory of balancing number technique determines Signals effectively.
3	Sujata Swain et al. [3]	2016	Lucas numbers, Fibonacci numbers, Lucas numbers, balancing numbers, and Lucas-balancing numbers etc	The method provides better accuracies of classifier and segmentation than other previous method.
4	Fatemeh Mohebalizadehgashtiet al. [4]	2016	A hybrid genetic algorithm	It can satisfy the assembly line with the synchronous conurbation.
5	A.P.Stakhov [5]	2006	Presented the Gazale formulas	The improved cryptographic method, which is a generalization of golden matrix.
6	Sergiy Koshkin et al. [6]	2017	Uses general unimodular matrices in place of the traditional *Q* matrices	We point out that golden cryptography is also generally unable to correct double errors in a single line of cipher text matrix.
7	Marghny H. et al. [7]	2014	Combination of haar wavelet and golden matrix.	This process has been provide multi security services in the signals
8	Prasanta Kumar Ray et al. [8]	2014	Used a new recurrence a Pell's equation	The results show accurate and effective.
9	A.P. Stakhov[9]	2014	Which are a wide generalization of the Binet and Pell number	Generalization of the Binet and Pell number
10	Ernatuti [10]	2010	Recurrence formula of the number of Extended Lucas Cube vertices	Better cryptographic protection of digital signals used in telecommunications, and also faster and easier to achieve.
11	Ray, Prasanta Kumar et al.[11]	2009	Pell and associated Pell numbers are very closely associated.	The balancing, co balancing and other related numbers are also expressible in terms of products of matrices
12	Monty Kester [12]	2010	Fibonacci sequence, in which each new number is the sum of the preceding two numbers.	Experimental results when different sequences and manipulations are performed on this sequence of numbers.

13	Mohammad Tahghighiet al.[13]	2010	K-Fibonacci number	This new proposed generalized cryptosystem based on k-Fibonacci numbers is more secure than the original golden cryptography against chosen plaintext attack.
14	Angel Martindel Rey et al. [14]	2010	Cryptosystem is trivially compromised.	It is not strong against a chosen-plaintext attack, which is a necessary cryptanalytic attack.
15	Prasanta Kumar et al. [15]	2015	The generating function in cryptography $g(x) = \sum_{n=0}^{\infty} a_n x^n$	The helpful in protection of digital signals.
16	Bijan kumarpatel et al. [16]	2009	Proposed new algorithm, such that $\{B_l, B_{l+1}\} \equiv \{0,1\}$ (mod m)	Find the periods of the balancing numbers modulo a product of consecutive Lucas-balancing numbers.
17	Marghny H et al. [17]	2014	Message Authentication Code (MAC) technique.	The provide authentication and the integrity of this scheme.
18	Fatima Amounas et al. [18]	2013	Elliptic curve using mealy machine and Fibonacci Q-matrix	To avoid the threat against possible attacks by hackers during transmission process of the message.
19	Sergiy Koshkin et al. [19]	2017	Uses general unimodular matrices in place of the traditional Q matrices	This unimodular cryptography is flexible for select Plaintext attacks that worked against golden cryptography
20	B. Krishna Gandhi et al. [20]	2012	Finite state machine and Pauli spins ½ matrices.	Finite state machines (FSM), also known as finite state automation (FSA), at their simplest, are models of the behaviors of a system.
21	Prasanta Kumar Ray et al. [21]	2014	using finite state machine	If we can be use four parameters then the level of security is very high.
22	B. Ravi Kumar et al [22]	2015	ElGamal encryption scheme	The Fibonacci Q-matrix is introduced as an elliptical curve and additional protection.
23	Licinius Dimitri Sa de Alcantara [23]	2017	Binary matrix encryption (BME) and formalized on a linear algebra basis.	This method can be performed on physical or application layer level, and can be easily applied into any digital storage and telecommunication system.
24	Ravi Kumar et al. [294]	2016	balancing-like and Lucas-balancing-like sequences	The helpful in protection of digital signals.
25	Mei-ChuChang [25]	2013	On a matrix product question in cryptography	$\lvert \boldsymbol{M_k(A,B)} \rvert > \frac{\mathbf{1}}{(\mathbf{16}_{\boldsymbol{d}}^{\boldsymbol{n}})(\mathbf{2(n-d)})^{\frac{\boldsymbol{n-d}}{\mathbf{2}}}} \; \boldsymbol{q}^{\min(\boldsymbol{n},\mathbf{2k-1})}$
26	Kalman Liptai [26]	2009	Baker-type Diophantine results and Bilu-Tichy theorem, respectively.	effective and ineffective finiteness statements for the balancing numbers
27	N. Taskara, et al. [27]	2010	Lucas numbers with binomial coefficients	The proposed method is protecting the signals.
28	KappagantuPrudhavi et al. [28]	2015	Reciprocals of Fibonacci numbers	Sum formulas with alternating signs are also studied

29	Ernastuti[29]	2014	Perfect Shuffle Crypto Algorithm (PSCA)	The PSCA is reasonably safe, especially for Chiprotext-only attacks. For a linear plaintext length of $N = 2^n$, it will take $O(N \log N)$ to decrypt both plain coding and ciphering text.
30	Raghu M. E et al. [30]	2015	Sequential and parallel method is analyzed	Modern cryptography techniques are virtually unbreakable, sometimes they also tend to attack

III. METHODOLOGY

At current time the role of cryptography are the major Encryption and decryption require the use of some secret information, commonly referred to as a key.

3.1. Fibonacci number

Fibonacci numbers are called numbers in the following integer sequence, which is called the Fibonacci sequence. The recurrence satisfied by the Fibonacci numbers is the arche type of a homogeneous linear recurrence relation with constant coefficients. Which sequence is called the Fibonacci sequence, defined as the recurrence relation are:

$\mathbf{F_{n+1}} = \mathbf{F_n} + \mathbf{F_{n-1}}$ .With the initial conditions are $F_1 = 1 \; and \; F_2 = 1$.

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

$$F^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (13)$$

$$F^1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (14)$$

3.2. 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 $\mathbf{P_{n+1}} = \mathbf{2P_n} + \mathbf{P_{n-1}}, \mathbf{n} \geq \mathbf{2}$

The recurrence relation of Pell Numbers is shown as:

$$P^n = \begin{cases} 0 & if \; n = 0 \\ 1 & if \; n = 1 \\ \mathbf{P_{n+1}} = \mathbf{2P_n} + \mathbf{P_{n-1}} & if \; n \geq 2 \end{cases} \ldots\ldots\ldots (15)$$

3.3. Fibonacci - Pell Transform

Fibonacci - Pell (FP) Transformation can be defined the mapping FB:$T^2 \rightarrow T^2$ such that

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \mathbf{F_i} & \mathbf{F_{i+1}} \\ \mathbf{P_i} & \mathbf{P_{i+1}} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\boldsymbol{mod N}) \; .$$

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

$$F_i \; is \; the \; i^{th} term \; of \; \; fibonacci \; series \; and \; P_i \; is \; the \; i^{th} Pell \; serie$$

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.

3.4. Affine transformation:

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

IV. PROPOSED WORK

The multi encryption methods are used in this algorithm and also Fibonacci- Pell Number as the first layer of encryption and affine transformation for super encryption.

3.5. Encryptionalgorithms

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

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

Step 2: Alice 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.

3.6. Decryptionalgorithms

Step 1: The super encrypted massage can be received by Bob

Step 2: Bob decrypts the super encrypted massage using:

$$E^{-1}(y) = \; a^{-1}(y - b)mod26 = (p^1)$$

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 $(FP) = \begin{pmatrix} F_1 & F_2 \\ P_1 & P_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots$ (16)

Encryptionalgorithms:

Step 1: Let the plane text

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

Step 2: Then we find the value

$C = p \times (FP)$ …….. (18)

$$C = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 22 & 40 \\ 27 & 47 \end{pmatrix} \ldots\ldots\ldots \quad (19)$$

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

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

Step 4: FREA is Encrypted message.

Decryptionalgorithms:

Step 1: FREA is First Decrypted message.

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
$(y-25)\text{mod}26$	22	14	1	21
First decrypted text	W	O	B	V

THEN $A_1 = \begin{pmatrix} W & O \\ B & V \end{pmatrix} = \begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix}$……(20)

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

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

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

$P = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} = \begin{pmatrix} E & S \\ H & U \end{pmatrix}$ …..…….. (22)

Case -2: For$i = 2$, Put them in Fibonacci - Pell $(FP) = \begin{pmatrix} F_2 & F_3 \\ P_2 & P_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$…… (23)

Encryptionalgorithms:

Step 1: Let the plane text

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

Step 2: Then we find the value

$C = p \times (FP)$ ……. ….. (25)

$C = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 40 & 98 \\ 47 & 114 \end{pmatrix}$….. (26)

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

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

Step 4: RVAX is Encrypted message.

Decryptionalgorithms:

Step 1: FREA is First Decrypted message.

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

THEN $A_1 = \begin{pmatrix} W & O \\ B & V \end{pmatrix} = \begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix}$ ..…… (27)

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

$\begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 30 & -8 \\ -19 & 20 \end{pmatrix}$…..... (28)

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

$P = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} = \begin{pmatrix} E & S \\ H & U \end{pmatrix}$ …….. (29)

This is a massage send and received by the Alice and Bob.

V. CONCLUSION AND FUTURE WORK

Fibonacci - Pell (FP) Transform can give sufficient results to secure the signals. The recurrence relation can be find sufficient results to secure the signals. Fibonacci - Pell (FP) Transform used for encryption and affine cipher can be used for super encryption. It ensures that to secure the data from attackers in this cryptographic method is fast and simple. In future we can be used the other method to check the security and the complexity of this transformation then we can say that Fibonacci - Pell (FP) Transform are more secure or not.

REFERENCES

1. Sudha K.R., Chandra Sekhar A., Reddy Prasad, Cryptography Protection of Digital Signals using Some Recurrence Relations. In IJCSNS VOL/ No- 7 /5 in 2007.
2. Prasanta Kumar Ray and PROF. G. K. Panda Balancing AND Cobalancing Numbers in 2014.
3. "Balancing and Lucas-Balancing Numbers and Their Application to Cryptography" in February 2016 by Swain Sujata, PratiharyChidananda and Ray Prasanta Kumar Computer Engineering and Applications Vol. 5, No. 1.
4. Fatemeh Mohebalizadehgashti, Professor F.M. Defersha Balancing, Sequencing and Determining the Number and Length of Workstations in a Mixed in Model Assembly Line April 2016.
5. StakhovA.P. "Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas functions, and the improved method of the golden cryptography" in 2006
6. Bani-Ahmad Feras, MohdTaibShatnawi, NedalTahat, SafaaShatnawi "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 in 2016.
7. TahghighiM., TuraevS., Jaafar A., MahmodR. and Md. M. Said "On the Security of Golden Cryptosystems" International Journal Contemp. Math. Sciences, Vol. 7, 2012, no. 7, 327 – 335
8. Chandra Sekhar A., Ch. Pragathi, Chaya Kumari D. and Kumar Ashok "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).
9. MOHAMMAD TAHGHIGHI SHARABYAN "On the Security of Golden Cryptosystems" International Journal Contemp. Math Sciences, Vol. 7, 2012.
10. Ernatuti, Ravi A, Sulistyo Salim"THE APPLICATION OF ELC NUMBER TO GOLDEN CRYPTOGRAPHY(GC)" The 5th International Conference on Information & Communication Technology and Systems IN 2011
11. Ray, Prasanta Kumar, Panda, G K "Balancing and Cobalancing Numbers". Ph.D. thesis on 29 Jun 2011.
12. Timothy Sprano, Jean Tweedy, Brenda Ayres "FIBONACCI SEQUENCE" Honors Program of Liberty University in 2012.
13. Mohammad Tahghighi, Azmi Jafaar, RamlanMahmod "Generalization of Golden Cryptography based on k-Fibonacci Numbers" in (ICINC) at 2010.

14. Thokchom Chhatrajit Singh "Lucas Numbers and Cryptography" NATIONAL INSTITUTE OF TECHNOLOGY ROURKELA, ORISSA-769008 IN 2012
15. Angel Martin Del Ray and Rodriguez Sanchez Gerardo "On the security of Golden cryptography" international journal of network security(IJNS). VOL7 IN Nov. 2007.
16. Prof David Joyner, "Projects in Cryptography, Codes, and Information Security" February 27, 2015
17. Ray Prasanta Kumar and SahuJuli "GENERATING FUNCTIONS FOR CERTAIN BALANCING AND LUCAS-BALANCING NUMBERS" Palestine Journal of Mathematics Vol. 5(2) (2016), 122–129
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.
19. Introduction of Fibonacci number jwilson.coe.uga.edu/EMT668/EMAT6680.
20. AmounasFatima, Hassan El,KinaniEl, Hajar Moha "Confidential Algorithm for Golden Cryptography Using Haar Wavelet" in (IJCSIS), Vol. 12, No. 8, August 2014.
21. Sergiy Koshkin, Taylor Styers "From golden to unimodular cryptography" Chaos, Solitons, and Fractals 105 (2017) 208–214
22. Gandhi B. Krishna, Sekhar A. Chandra, Sri Lakshmi S. "Encryptions of Data Streams using Pauli Spin ½ Matrices and Finite State Machine" IN journals IJCA Volume no. 37– No.2, 05/01/ 2012.
23. Application of Some Recurrence Relations to Cryptography using Finite State Machine" by Ray Prasanta Kumar, Krishna DilaGopal, and Patel Bijan Kumar in (IJCSEE) Volume 2, Issue no.4 in 2014.
24. Incomplete Lucas - Balancing Numbers And Balancing Numbers by Patel Bijan Kumar, Irmak Nurettin and Ray Prasanta Kumar in Math Reports (70), 1 jan (2018).
25. Licinius Dimitri Sa de Alcantar Towards a simple and secure method for binary cryptography via linear algebraRevistaBrasileira de ComputacaoAplicada (ISSN 2176-6649), Passo Fundo, v. 9, n. 3, p. 44-55, out. 2017
26. DavalaRavi Kumar and Panda G. K. "On sum and ratio formulas for balancing-like sequences" Print ISSN 1310–5132, Vol. 22, 2016, No. 3.
27. Mei-Chu Chang On a matrix product question in cryptography Linear Algebra and its Applications 439(2013).
28. Kalman Liptai, Florian Luca, Pinter Akos and SzalayLaszlo Generalized balancing numbers Indag. Mathem., N.S., page 87–100 in 2009
29. KappagantuPrudhavi Nag and Professor G. K. Panda "SUM OF PRODUCT OF RECIPROCALS OF FIBONACCI NUMBERS" National Institute of Technology, Rourkela May 2015
30. Ernastuti "PERFECT SHUFFLE ALGORITHM FOR CRYPTOGRAPHY"ARPN Journal of Engineering and Applied Sciences VOL. 9, NO. 12, DEC. 2014.

AUTHOR'S DESCRIPTION:

I **Esh Narayan** was born in 20 Feb. 1984. I have completed my Post Graduation (M.Tech) in Computer Science and Engineering has been completed from LPU Punjab in 2012. Present time I am working in Prabhat Engineering College as an Assistant Professor in Computer Science and Engineeringdepartment since Aug. 2012.
I am doing Ph.D from IFTM University Moradabad under the excellent guidance of Dr. Abhishek Mishra (Batch-2018) with topic **"cryptography protection of digital signals using recurrence relations with golden matrix**"completed three RDC and course work successfully.

I**Abhishek Mishra** completed myPost Graduation (M.Tech) in Computer Science and Engineering from RGPV University Bhopal in 2008. Present time I am working in Associate Professor, Computer Science and Engineering, IFTM University, Moradabadin Aug. 2008.

I **Sunil Kumar Singh** was born in 19 Oct 1985. I have completed my Post Graduation (M.Tech) in Electrical Engineering has been completed from CMJ University Meghalaya in 2012 and topic was **"Automatic Solar Power Tracking".** Present time I am working in Prabhat Engineering College as an Assistant Professor in Electrical Engineering and also handle Principal post in Diploma section since Aug. 2014. I am doing Ph.D from IFTM University Moradabad under the excellent guidance of Dr. Anil Kumar (batch-2018) with topic **"Applications of ANN and Fuzzy Logic Technique for Cost Effective Solution for Photovoltaic Systems",** completed three RDC and course work successfully.