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 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, Prathiyarab Chidananda and Ray Prasanta Kumar (2016) method is well known that, recursive relation for the sequence \( a_0, a_1, a_2, a_3, a_4, \ldots, a_n \), are an equation that relates to certain of its preceding terms \( a_0, a_1, a_2, a_3, a_4, \ldots, a_n \). Initial conditions for the sequence \( a_0, a_1, a_2, a_3, a_4, \ldots \) 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:

\[
Q^{2x} = \begin{pmatrix} cFs(2x + 1) & sFs(2x) \\ sFs(2x) & cFs(2x - 1) \end{pmatrix} \quad (1)
\]

\[
Q^{2x+1} = \begin{pmatrix} cFs(2x + 2) & sFs(2x + 1) \\ sFs(2x + 1) & cFs(2x) \end{pmatrix} \quad (2)
\]

Where

\[
sFs(x) = \frac{\tau^x - \tau^{-x}}{\sqrt{5}}, \quad cFs(x) = \frac{\tau^x + \tau^{-x}}{\sqrt{5}} \quad (3)
\]

The equations 1 and 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. We can use 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:

\[
L_{k+1} = L_k + L_{k-1} \quad (4)
\]

With the initial condition \( L_0 = 2, L_1 = 1 \)

\[
L^n = \begin{pmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{pmatrix} \quad (5)
\]

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

Where \( n = 1, 2, 3 \ldots \)

\[
L^1 = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \quad (7)
\]

These are the \((2 \times 2)\) matrix

LUCAS BALANCING NUMBER

This is the recurrence formula of Lucas-balancing numbers \( C_n \), then \( C_n^2 = 8B_n^2 + 1 \)

\[
C_{n+1} = 6C_n - C_{n-1} \quad (8)
\]

The initial condition \( C_1 = 3, C_2 = 17 \)

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

BALANCING NUMBER

This is the recurrence formula of balancing number \( B_n \), then \( B_{n+1} = 6B_n - B_{n-1} \). Where \( B_n \) is a balancing number with initial Condition?

\[
B^n = \begin{pmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{pmatrix} \quad (10)
\]

Then

\[
B^1 = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix} \quad (11)
\]

But extended balancing number is

\[
B^n = \begin{pmatrix} -B_{n-1} & -B_n \\ B_n & B_{n+1} \end{pmatrix} \quad (12)
\]

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.

Revised Manuscript Received on December 25, 2020.

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

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication
For $k \in \mathbb{Z}^+$, it’s denoted by $M_k(A, B) := \{ f(A)g(B) : f, g \in \mathbb{F}_q[x], \text{deg } f, \text{deg } g = k \}$, Assu \geq 2n

we prove that $|M_k(A, B)| > 4^{-k}q^{\min\{n,2k-1\}}$. Moreover, let $d = \dim \ker((AB - BA)$, then we prove that

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

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

$$x^k + 2x^{k-1} + \ldots + (1-x)^k = (x + 1)^l + \ldots + (y - 1)^l$$

For fixed positive integers $k$ and $l$, Prakash Kumar Ray and Prof. G.K. 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, Ramlan Mahmoud (2010), Mohamad Rushdan Md. has proposed a new kind of crypto-system 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 Jula Sahu 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 ciphers Generation 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. Panda et 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       | Marghy 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. |
| No. | Author(s) | Year | Description |
|-----|-----------|------|-------------|
| 14  | Angel Martindel Rey et al. [14] | 2010 | Cryptosystem is trivially compromised. |
| 15  | Prasanta Kumar et al. [15] | 2015 | The generating function in cryptography \( g(x) = \sum_{n=0}^{\infty}a_nx^n \) |
| 16  | Bijan kumarpatel et al. [16] | 2009 | Proposed new algorithm, such that \( B_p, B_{i+1} \equiv \{0,1\} \) (mod m) |
| 17  | Marghny H et al. [17] | 2014 | Message Authentication Code (MAC) technique. |
| 18  | Fatima Amounas et al. [18] | 2013 | Elliptic curve using mealy machine and Fibonacci Q-matrix |
| 19  | Sergiy Koshkin et al. [19] | 2017 | Uses general unimodular matrices in place of the traditional Q matrices |
| 20  | B. Krishna Gandhi et al. [20] | 2012 | Finite state machine and Pauli spins ½ matrices. |
| 21  | Prasanta Kumar Ray et al. [21] | 2014 | Using finite state machine |
| 22  | B. Ravi Kumar et al [22] | 2015 | ElGamal encryption scheme |
| 23  | Licinius Dimitri Sa de Alcantara [23] | 2017 | Binary matrix encryption (BME) and formalized on a linear algebra basis. |
| 24  | Ravi Kumar et al. [294] | 2016 | Balancing-like and Lucas-balancing-like sequences |
| 25  | Mei-ChuChang [25] | 2013 | On a matrix product question in cryptography |
| 26  | Kalman Liptai [26] | 2009 | Baker-type Diophantine results and Bilu-Tichy theorem, respectively. |
| 27  | N. Taskara, et al. [27] | 2010 | Lucas numbers with binomial coefficients |
| 28  | KappagantuPrudhavi et al. [28] | 2015 | Reciprocals of Fibonacci numbers |
| 29  | Ernastuti[29] | 2014 | Perfect Shuffle Crypto Algorithm (PSCA) |
| 30  | Raghu M. E et al. [30] | 2015 | Sequential and parallel method is analyzed |
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 archetypal type of a homogeneous linear recurrence relation with constant coefficients. Which sequence is called the Fibonacci sequence, defined as the recurrence relation are:

\[ F_{n+1} = F_n + F_{n-1} \]

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…….

\[ F^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \] (13)

\[ P^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \] if \( n = 0 \)
\[ P^n = \begin{pmatrix} 2P_n & P_{n-1} \end{pmatrix} \] if \( n \geq 2 \) (15)

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 \( P_{n+1} = 2P_n + P_{n-1}, n \geq 2 \)

The recurrence relation of Pell Numbers is shown as:

\[ P^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \] if \( n = 0 \)
\[ P^n = \begin{pmatrix} 2P_n & P_{n-1} \end{pmatrix} \] if \( n \geq 2 \) (15)

3.3. Fibonacci - Pell Transform

Fibonacci - Pell (FP) Transformation can be defined the mapping \( \mathbb{F} \mathbb{B} \mathbb{T}^2 \rightarrow \mathbb{T}^2 \) such that

\[ \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} F_i & F_{i+1} \\ P_i & P_{i+1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N \]

Where \( x, y \in \{0,1,2,\ldots,N-1\} \) in this transformation where \( F_i \) is the \( i^{th} \) term of Fibonacci series and \( P_i \) is the \( i^{th} \) Pell serie

Denoting \( \begin{pmatrix} F_i & F_{i+1} \\ P_i & P_{i+1} \end{pmatrix} \) These transformations continue in this way.

3.4. Affine transformation:

We can use 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 use \( P = a^{-1}(y - b)\mod N \)

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. Encrypoticalgorithms

Step 1: Let the plain text \( A \) be a square matrix of orde, \( n > 0 \). Let \( A_1 \) be the choice of \( i^{th} \) permutation. Then Alice creates:

Plain text: \( p = p_1, p_2, \ldots, p_n \).

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

Step 3: Then Alice performs encryption with C to affine transformation is \( E(x) = (ax + b)\mod N \)

\( \gcd(a, N) = 1 \) and a and b are secret key.

Step 4: Alice sends super encrypted message to Bob.

3.6. Decryptionalgorithms

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

Step 2: Bob decrypts the super encrypted message using:

\[ E^{-1}(y) = a^{-1}(y - b)\mod 26 = (p^1) \]

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

Example:

Case 1: \( \text{for } i = 1 \), Put them in Fibonacci - Pell (FP) =

\[ \begin{pmatrix} F_1 & F_2 \\ P_1 & P_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \] (16)

Encryptionalgorithms:

Step 1: Let the plane plaintext

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

Step 2: Then we find the value

\[ C = p \times (FP) \]

\[ \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 22 & 40 \\ 27 & 47 \end{pmatrix} \] (19)

Step 3: Now we can be used affine transformation \( E(x) = (ax + b)\mod 26 \) for \( a = 5, b = 25 \)

| x | 22 | 40 | 27 | 47 |
|---|---|---|---|---|
| xmod26 | 22 | 14 | 1 | 21 |
| 5x + 25 | 135 | 95 | 30 | 130 |
| (5x + 25)mod26 | 5 | 17 | 4 | 0 |

Message \( F \) R E A

Step 4: FREA is Encrypted message.

Decryptionalgorithms:

Step 1: FREA is First Decrypted message.

Step 2: Compute the inverse affine transform \( E^{-1}(y) = a^{-1}(y - b)\mod 26 \)

| 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

THEN \( A_1 = \begin{pmatrix} W & 0 \\ B & V \end{pmatrix} = \begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix} \) (20)

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

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

| Value | 30 | -8 | -19 | 20 |
|---|---|---|---|---|
| mod26 | 4 | 18 | 7 | 20 |

Second Decrypted Text \( E \) S H U
Cryptography Protection of Digital Signals using Fibonacci - Pell Transformation via Golden Matrix

\[ P = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} = \begin{pmatrix} E & S \\ H & U \end{pmatrix} \] \hspace{1cm} (22)

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

Encryptionalgorithms:

Step 1: Let the plane text
\[ A = \begin{pmatrix} E & S \\ H & U \end{pmatrix} = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} \] \hspace{1cm} (24)

Step 2: Then we find the value
\[ C = p \times (FP) \] \hspace{1cm} (25)

\[ C = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 40 & 98 \\ 47 & 114 \end{pmatrix} \] \hspace{1cm} (26)

Step 3: Now we can be used affine transformation \( E(x) = (ax + b) \mod 26 \) 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 |

Step 4: RVAX is Encrypted message.

Decryptionalgorithms:

Step 1: FREA is First Decrypted message.

Step 2: Compute the inverse affine transform \( E^{-1}(y) = a^{-1}(y - b) \mod 26 \)

| x | R | V | A | X |
|---|---|---|---|---|
| y | 17 | 21 | 0 | 23 |
| y - 25 | -8 | -4 | -25 | -2 |
| 21(y - 25) | -168 | -84 | -525 | -42 |
| (y - 25)mod26 | 14 | 20 | 21 | 10 |

First decrypted text

THEN \( A_1 = \begin{pmatrix} W & 0 \\ B & V \end{pmatrix} = \begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix} \) \hspace{1cm} (27)

Step 3: Bob compute \( p = p' \times (FB)^{-1} \mod 26 \)

\[ \begin{pmatrix} 22 & 14 \\ 1 & 21 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 30 & -6 \\ -19 & 20 \end{pmatrix} \] \hspace{1cm} (28)

Value

| 30 | -8 | -19 | 20 |
|---|----|-----|----|
| mod26 | 4 | 18 | 7 | 20 |

Second Decrypted Text

\[ P = \begin{pmatrix} 4 & 18 \\ 7 & 20 \end{pmatrix} = \begin{pmatrix} E & S \\ H & U \end{pmatrix} \] \hspace{1cm} (29)

This is a message 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 IJCNSS 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 Mohebalzadehagholi, 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. “Gazelle 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, MohdTabShatnawi, NedaTahat, 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. TahgihguM, 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: 2278-5788, 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. Emrattutti, Ravi A., Sulisoth 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 Sahulul "GENERATING FUNCTIONS FOR CERTAIN BALANCING AND LUCAS-BALANCING NUMBERS" Palestine Journal of Mathematics Vol. 5(2) (2016), 122-129
18. BJIAN KUMAR PATEL, SHANTA KUMARI SUNANDA, and PRASANTA KUMAR RAY "PERIOD OF BALANCING NUMBERS MODULO PRODUCT OF CONSECUTIVE LUCAS-BALANCING NUMBERS" MATHEMATICA, 60 (93), No 2, 2018.
19. Introduction of Fibonacci number jwilton.coe.uga.edu/EMAT6680/EMAT6680.
20. AmounasFatima, Hassan EL,KinaniEL, Hajar Moha “Confidential Algorithm for Golden Cryptography Using Haar Wavelet” in (ICSEIS), 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 ComputacaooAplicada (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 1510–5132, 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. Ernstusiti “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 Engineering department 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 my Post 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, Moradabad in 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 CMU 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.