Tikrit Journal of Pure Science
ISSN: 1813 – 1662 (Print) --- E-ISSN: 2415 – 1726 (Online)
Journal Homepage: http://tjps.tu.edu.iq/index.php/j

New Technique using Fibonacci Matrices with Play-Fair System in Cryptography

Awni M.Gaftan , Akram S.Mohammed, Salah F.Tarfa
Department of Mathematics , College of Computer Science and Mathematics ,. Tikrit University , Tikrit , Iraq
https://doi.org/10.25130/tjps.v27i2.70

ARTICLE INFO.
Article history:
-Received: 30 / 11 / 2021
-Accepted: 22 / 12 / 2021
-Available online: / / 2022
Keywords: Fibonacci sequences, play-Fair method, Cryptography, Fibonacci key Generation, cipher, Encryption
Corresponding Author:
Name: Awni M.Gaftan
E-mail:
Tel:

ABSTRACT

In this paper we introduce a new Technique, this technique depends on the Fibonacci sequence and Fibonacci Matrices with a Play- Fair which is one of the cryptography systems. This method is applied in two steps, in the first step we generate the Fibonacci matrices with key matrix by particularity Fibonacci sequence to obtain first cipher and the second step we apply the Play-Fair method to obtain the 2nd cipher (final cipher).

Introduction

The Fibonacci's numbers sequence (1,1,2,3,5,8,13,21,34…)this sequence can be generate by the following formula[3]:

$f_{n+2} = f_{n+1} + f_n \quad \forall\, n \in N^* \quad f_1 = f_2 = 1$

Where:

1. f_{3n-2} , f_{3n-1} are an odd number and f_{3n} is even number $\forall\, n \in N^*$.
2. $f_{n+1}^2 - f_n f_{n+2} = (-1)^n$
3. Also, we obtain the Fibonacci's matrix as:
4. $Q_{(2x2)}^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$

Fibonacci numbers appear in Nature so frequently that they can be considered as Nature's Perfect Numbers. Also, another important Nature's number, the Golden ratio, which seen, in every area of life and art, and usually it is associated with aesthetics, is related to Fibonacci sequence[6].

In 2020, Kalika P. and Hrishikish M. are using Fibonacci matrices with Affine-Hill cipher in cryptography [1]. Moh Vasim and etal.. in (2018) are improved Play-Fair encryption technique with Fibonacci sequences to obtain good and secrete key [2].

Definition: Generate A Matrix Key [7]

The basic working principle of this methods is also done by two people (user), we will use matrixes instead of numbers and find the public key and then by using certain equation, both users will get the same key.

Definition: **Fibonacci Sequence and Fibonacci Q_ Matrix**

The Fibonacci sequence [7,8,9] is the sequence of integers fn, defined by the recurrence relation

$f_{n+2} = f_{n+1} + f_n \quad \forall\, n \in N^* \; f_0 = 0 \; f_1 = f_2 = 1$

5. Fibonacci-Q_λ _ matrix was introduced by Brenner [7], later King were enumerated it's basic properties. In 1985, Honsberger [7] showed that the Fibonacci Q-matrix is a squarematrix of order 2 of the form

$Q_2 = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$

1. The Algorithm:

Now, we introduce the algorithm for the new method , in which we join between the Fibonacci matrices sequence with the classical play-Fair cryptosystem:

Encryption:

Chose a nonprintable character(@,&,*,#,…..) to insert it in the spaces among the words in plain text or to complete the matrix.

Divide the plain text into equal segments (every segment contain four characters or letters) these segments are represented as matrix (2X2).

Using the following table of codes for alphabet:

Table (a) Alphabet codes

-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	-11	-12	-13	-14
26	25	24	23	22	21	20	19	18	17	16	15	14	13
A	B	C	D	E	F	G	H	I	J	K	L	M	N
-15	-16	-17	-18	-19	-20	-21	-22	-23	-24	-25	-26	-27	
12	11	10	9	8	7	6	5	4	3	2	1	0	
O	P	Q	R	S	T	U	V	W	X	Y	Z	δ	

1. Generate the key matrix by Fibonacci formula (f_{00}=0,f_{01}=1,f_{02}=1,f_{03}=2,f_{04}=3,f_{05}=5,f_{06}=8,f_{07}=13, f_{08}=21,f_{09}=34,f_{10}=55)
2. Cipher 1= (plain matrix + Key matrix) mod n.
3. Cipher 2: we apply the Play-Fair method:

Table (b) Play-Fair Table

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

a. Decryption:

The decryption begin with cipher 2 and we apply the play-fair but in reverse motion to obtain cipher 1. And we use the key matrix with cipher 1 (with mod n) to obtain plain text.

Particular part:

Now, we apply the algorithm in the following example:

Plaintext: (Corn Finger Filled Chocolate Cream)

With symbol (δ) and divide it into segments the plain text is become:

Corn δFin $ger\delta$ Fill edδC hoco late δCre am$\delta\delta$

And with the table of codes and put the codes in matrices (2X2) as below:

$$\text{Corn} = \begin{bmatrix} C & o \\ r & n \end{bmatrix} = \begin{bmatrix} 4 & 22 \\ 15 & 24 \end{bmatrix}$$

$$\delta Fin = \begin{bmatrix} \delta & F \\ i & n \end{bmatrix} = \begin{bmatrix} 0 & 21 \\ 18 & 13 \end{bmatrix}$$

$$ger\delta = \begin{bmatrix} g & e \\ r & \delta \end{bmatrix} = \begin{bmatrix} 20 & 22 \\ 9 & 0 \end{bmatrix}$$

$$Fill = \begin{bmatrix} F & i \\ l & l \end{bmatrix} = \begin{bmatrix} 21 & 18 \\ 15 & 15 \end{bmatrix}$$

$$\text{ed}\delta\text{C} = \begin{bmatrix} e & d \\ \delta & C \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 0 & 24 \end{bmatrix}$$

$$\text{hoco} = \begin{bmatrix} h & o \\ c & o \end{bmatrix} = \begin{bmatrix} 19 & 12 \\ 24 & 12 \end{bmatrix}$$

$$\text{late} = \begin{bmatrix} l & a \\ t & e \end{bmatrix} = \begin{bmatrix} 18 & 26 \\ 7 & 22 \end{bmatrix}$$

$$\delta Cre = \begin{bmatrix} \delta & C \\ r & e \end{bmatrix} = \begin{bmatrix} 0 & 24 \\ 9 & 22 \end{bmatrix}$$

$$\text{am}\delta\delta = \begin{bmatrix} a & m \\ \delta & \delta \end{bmatrix} = \begin{bmatrix} 26 & 14 \\ 0 & 0 \end{bmatrix}$$

Now, to generate the key matrix from the Fibonacci sequence:

where n=1 and $Q^{n}_{(2x2)} = Q^{11}_{(2X2)}$

Then,

(f_{00}=0,f_{01}=1,f_{02}=1,f_{03}=2,f_{04}=3,f_{05}=5,f_{06}=8,f_{07}=13, f_{08}=21,f_{09}=34,f_{10}=55)

and so the key matrix is:

$$Q^{11}_{(2X2)} = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix} = \begin{bmatrix} f_{12} & f_{11} \\ f_{11} & f_{10} \end{bmatrix} = \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}$$

and add the key matrix to all plain matrices with Mod. Function (mod 27)

$$\text{Corn} = \left(\begin{bmatrix} 24 & 12 \\ 9 & 13 \end{bmatrix} + \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}\right)(mod27) = \begin{bmatrix} 168 & 101 \\ 98 & 68 \end{bmatrix}(mod27)$$

$$= \begin{bmatrix} 168\text{mod}_{27} & 101\text{mod}_{27} \\ 98\text{mod}_{27} & 68\text{mod}_{27} \end{bmatrix} = \begin{bmatrix} 6 & 20 \\ 17 & 14 \end{bmatrix} = \text{UGJM}$$

$$\delta Fin = \left(\begin{bmatrix} 0 & 21 \\ 18 & 13 \end{bmatrix} + \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}\right)(mod27) = \begin{bmatrix} 144 & 110 \\ 107 & 68 \end{bmatrix}(mod27)$$

$$= \begin{bmatrix} 144\text{mod}_{27} & 110\text{mod}_{27} \\ 107\text{mod}_{27} & 68\text{mod}_{27} \end{bmatrix} = \begin{bmatrix} 9 & 2 \\ 26 & 14 \end{bmatrix} = \text{RYAM}$$

$$ger\delta = \left(\begin{bmatrix} 20 & 22 \\ 9 & 0 \end{bmatrix} + \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}\right)(mod27) = \begin{bmatrix} 164 & 111 \\ 98 & 55 \end{bmatrix}(mod27)$$

$$= \begin{bmatrix} 164\text{mod}_{27} & 111\text{mod}_{27} \\ 98\text{mod}_{27} & 55\text{mod}_{27} \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 17 & 1 \end{bmatrix} = \text{YXJZ}$$

$$Fill = \left(\begin{bmatrix} 21 & 18 \\ 15 & 15 \end{bmatrix} + \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}\right)(mod27) = \begin{bmatrix} 165 & 107 \\ 104 & 70 \end{bmatrix}(mod27)$$

$$= \begin{bmatrix} 165\text{mod}_{27} & 107\text{mod}_{27} \\ 104\text{mod}_{27} & 70\text{mod}_{27} \end{bmatrix} = \begin{bmatrix} 3 & 26 \\ 23 & 16 \end{bmatrix} = \text{XADK}$$

$$ed\delta C = \left(\begin{bmatrix} 22 & 23 \\ 0 & 24 \end{bmatrix} + \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}\right)(mod27) = \begin{bmatrix} 166 & 112 \\ 89 & 79 \end{bmatrix}(mod27)$$

$$= \begin{bmatrix} 166\text{mod}_{27} & 112\text{mod}_{27} \\ 89\text{mod}_{27} & 79\text{mod}_{27} \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 8 & 25 \end{bmatrix} = \text{WWSB}$$

$$\text{hoco} = \left(\begin{bmatrix} 19 & 12 \\ 24 & 12 \end{bmatrix} + \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}\right)(mod27) = \begin{bmatrix} 163 & 101 \\ 113 & 67 \end{bmatrix}(mod27)$$

$$= \begin{bmatrix} 163\text{mod}_{27} & 101\text{mod}_{27} \\ 113\text{mod}_{27} & 67\text{mod}_{27} \end{bmatrix} = \begin{bmatrix} 1 & 20 \\ 5 & 13 \end{bmatrix} = \text{ZTVN}$$

$$\text{late} = \left(\begin{bmatrix} 18 & 26 \\ 7 & 22 \end{bmatrix} + \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}\right)(mod27) = \begin{bmatrix} 162 & 115 \\ 96 & 77 \end{bmatrix}(mod27)$$

$$= \begin{bmatrix} 162\text{mod}_{27} & 115\text{mod}_{27} \\ 96\text{mod}_{27} & 77\text{mod}_{27} \end{bmatrix} = \begin{bmatrix} 0 & 7 \\ 15 & 23 \end{bmatrix} = \delta TLD$$

$$\delta Cre = \left(\begin{bmatrix} 0 & 24 \\ 9 & 22 \end{bmatrix} + \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}\right)(mod27) = \begin{bmatrix} 144 & 113 \\ 98 & 77 \end{bmatrix}(mod27)$$

$$= \begin{bmatrix} 144\text{mod}_{27} & 113\text{mod}_{27} \\ 98\text{mod}_{27} & 77\text{mod}_{27} \end{bmatrix} = \begin{bmatrix} 9 & 5 \\ 17 & 23 \end{bmatrix} = \text{RVJD}$$

$$am\delta\delta = \left(\begin{bmatrix} 26 & 14 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 144 & 89 \\ 89 & 55 \end{bmatrix}\right)(mod27) = \begin{bmatrix} 170 & 103 \\ 89 & 55 \end{bmatrix}(mod27)$$

$$= \begin{bmatrix} 170\text{mod}_{27} & 103\text{mod}_{27} \\ 89\text{mod}_{27} & 55\text{mod}_{27} \end{bmatrix} = \begin{bmatrix} 8 & 22 \\ 8 & 1 \end{bmatrix} = \text{SHSD}$$

The first cipher (C1)

= (UGJMRYAMYXJZXADKWWSZZTVNδTLDUVJDSHSD)
Suppose that (δ = A , W = B) The symbols are agreed upon to get :-
= (UGJMRYAMYXJZXADKBWSZZTVNATLDRVJDSHSD)
To produce the second cipher (C2) we apply the Play-Fair method (table-2) but we start with key word put it in the table and complete the alphabet:
- Let the key word is (Matrix), then the table of Play-fair is:-

M	**A**	**T**	**R**	**I**
X	**B**	**C**	**D**	**E**
F	**G**	**H**	**J/K**	**L**
N	**O**	**P**	**Q**	**S**
U	**V**	**W**	**Y**	**Z**

The work of this table is depend on the position of the letter and the (left/right) and (up/ down) and the cross:
UG:FV,JM:FR,RY:DR,AM:MT,YX:UD,JZ:LY,XA: MB, DK: KQ,BW:CV
SB:OE,ZT:WI,VN:UO,AT:TR,LD:JE,RV:AY,JD:QJ, SH:DL,SD:QE

Decryption

FV:UG
,FR:JM,DR:RY,MT,AM,UD:YX,YL:JZ,MB:XA,KQ :DK,CV:BW
OE:SB,WI:ZT,UO:VN,TR:AT,JE:LD,AY: RV,QJ:JD,DL:SH,QE:SD
So the second cipher (C2) is:-
(UGJMRYAMYXJZXADKBWOEZTVNATLDRVJDSHSD)
Let's get the ciphertext after offset (δ = A , W = B) :-
(**UGJMRYAMYXJZXADKWWOBZTVNδTLDRVJDSHSD**)

Decryption

After we apply the reverse motion of play-fair:

$$\text{UGJM} = \left(\begin{bmatrix}6 & 20\\ 17 & 14\end{bmatrix} - \begin{bmatrix}144 & 89\\ 89 & 55\end{bmatrix}\right)(\text{mod}_{27}) = \begin{bmatrix}-138 & -69\\ -72 & -41\end{bmatrix}(mod_{27}) =$$
$$= \begin{bmatrix}-138(\text{mod}_{27}) & -69(\text{mod}_{27})\\ -71(\text{mod}_{27}) & -41(\text{mod}_{27})\end{bmatrix} = \begin{bmatrix}24 & 12\\ 9 & 13\end{bmatrix} = \text{Corn}$$

$$\text{RYAM} = \left(\begin{bmatrix}9 & 2\\ 26 & 14\end{bmatrix} - \begin{bmatrix}144 & 89\\ 89 & 55\end{bmatrix}\right)(\text{mod}_{27}) = \begin{bmatrix}-135 & -87\\ -63 & -41\end{bmatrix}(\text{mod}_{27})$$
$$= \begin{bmatrix}-135(\text{mod}_{27}) & -87(\text{mod}_{27})\\ -63(\text{mod}_{27}) & -41(\text{mod}_{27})\end{bmatrix} = \begin{bmatrix}0 & 21\\ 18 & 13\end{bmatrix} = \delta Fin$$

$$\text{YXJZ} = \left(\begin{bmatrix}2 & 3\\ 17 & 1\end{bmatrix} - \begin{bmatrix}144 & 89\\ 89 & 55\end{bmatrix}\right)(\text{mod}_{27}) = \begin{bmatrix}-142 & -86\\ -72 & -54\end{bmatrix}(\text{mod}_{27})$$
$$= \begin{bmatrix}-142(\text{mod}_{27}) & -86(\text{mod}_{27})\\ -72(\text{mod}_{27}) & -54(\text{mod}_{27})\end{bmatrix} = \begin{bmatrix}20 & 22\\ 9 & 0\end{bmatrix} = \text{ger}\delta$$

$$\text{XADK} = \left(\begin{bmatrix}3 & 26\\ 23 & 16\end{bmatrix} - \begin{bmatrix}144 & 89\\ 89 & 55\end{bmatrix}\right)(\text{mod}_{27}) = \begin{bmatrix}-141 & -63\\ -66 & -39\end{bmatrix}(\text{mod}_{27})$$
$$= \begin{bmatrix}-141(\text{mod}_{27}) & -63(\text{mod}_{27})\\ -66(\text{mod}_{27}) & -39(\text{mod}_{27})\end{bmatrix} = \begin{bmatrix}21 & 8\\ 15 & 15\end{bmatrix} = \text{Fill}$$

$$\text{WWSZ} = \left(\begin{bmatrix}4 & 4\\ 8 & 25\end{bmatrix} - \begin{bmatrix}144 & 89\\ 89 & 55\end{bmatrix}\right)(\text{mod}_{27}) = \begin{bmatrix}-140 & -85\\ -81 & -30\end{bmatrix}(\text{mod}_{27})$$
$$= \begin{bmatrix}-140(\text{mod}_{27}) & -85(\text{mod}_{27})\\ -81(\text{mod}_{27}) & -30(\text{mod}_{27})\end{bmatrix} = \begin{bmatrix}22 & 23\\ 0 & 24\end{bmatrix} = \text{ed}\delta\text{c}$$

$$\text{ZTUN} = \left(\begin{bmatrix}1 & 20\\ 5 & 13\end{bmatrix} - \begin{bmatrix}144 & 89\\ 89 & 55\end{bmatrix}\right)(\text{mod}_{27}) = \begin{bmatrix}-143 & -69\\ -84 & -42\end{bmatrix}(\text{mod}_{27})$$
$$= \begin{bmatrix}-143(\text{mod}_{27}) & -69(mod_{27})\\ -84(\text{mod}_{27}) & -42(\text{mod}_{27})\end{bmatrix} = \begin{bmatrix}19 & 12\\ 24 & 12\end{bmatrix} = \text{hoco}$$

$$\delta\text{TLD} = \left(\begin{bmatrix}0 & 7\\ 15 & 23\end{bmatrix} - \begin{bmatrix}144 & 89\\ 89 & 55\end{bmatrix}\right)(\text{mod27}) = \begin{bmatrix}-144 & -82\\ -74 & -22\end{bmatrix}(\text{mod27})$$
$$= \begin{bmatrix}-144(\text{mod}_{27}) & -82(\text{mod}_{27})\\ -74(\text{mod}_{27}) & -22(\text{mod}_{27})\end{bmatrix} = \begin{bmatrix}18 & 26\\ 7 & 22\end{bmatrix} = \text{iate}$$

$$\text{RVJD} = \left(\begin{bmatrix}9 & 5\\ 17 & 23\end{bmatrix} - \begin{bmatrix}144 & 89\\ 89 & 55\end{bmatrix}\right)(\text{mod}_{27}) = \begin{bmatrix}-135 & -84\\ -72 & -32\end{bmatrix}(\text{mod}_{27})$$
$$= \begin{bmatrix}-135(\text{mod}_{27}) & -84(\text{mod}_{27})\\ -72(\text{mod}_{27}) & -32(\text{mod}_{27})\end{bmatrix} = \begin{bmatrix}0 & 24\\ 9 & 22\end{bmatrix} = \delta\text{Cre}$$

$$\text{SHSD} = \left(\begin{bmatrix}8 & 22\\ 8 & 1\end{bmatrix} - \begin{bmatrix}144 & 89\\ 89 & 55\end{bmatrix}\right)(\text{mod}_{27}) = \begin{bmatrix}-136 & -67\\ -81 & -54\end{bmatrix}(\text{mod}_{27})$$
$$= \begin{bmatrix}-136(\text{mod}_{27}) & -67(\text{mod}_{27})\\ -81(\text{mod}_{27}) & -54(\text{mod}_{27})\end{bmatrix} = \begin{bmatrix}26 & 14\\ 0 & 0\end{bmatrix} = \text{am}\delta\delta$$

So we see the plain text is more great than the original plain text and this indicate that the cipher text is different from the original cipher text and we have (the first plain text) as fellow:
(CornδFingerδFilledδhocoiateδCream$\delta\delta$)
And by the cancel the symbol (δ) we obtain the original plain text :
(Corn Finger Filled Chocolate Cream)

References

[1] Kalika Prasad, Hrishikesh Mahato, (2020), (Cryptography using generalized Fibonacci matrices with Affine-Hill cipher), *arXiv*:.11936v1 [cs.CR] 25.

[2] Mohd Vasim Ahamad, Misbah Urrahman Siddiqui, Maria Masroor, Urooj Fatima, (2018) , (An Improved Playfair Encryption Technique Using Fibonacci Series Generated Secret Key). *International Journal of Engineering & Technology*, **7 (4.5)** 347-351.

[3] Dr. Ing. Edward Opoku-Mensah, Abilimi A. Christopher, Francis Ohene Boateng, (2013), (Comparative Analysis of Efficiency of Fibonacci Random Number Generator Algorithm and Gaussian Random Number Generator Algorithm in a Cryptographic System), *Computer Engineering and Intelligent Systems* ,**ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online),** Vol.4, No.10,.

[4] A. Joseph Raphael, Dr. V. Sundaram, (2012), (Secured Communication through Fibonacci Numbers and Unicode Symbols), *International Journal of Scientific & Engineering Research*, **Volume 3, Issue 4, , ISSN 2229-5518. 1-5,**

[5] Özvatan, M., & Pashaev, O. K. (2017). Generalized Fibonacci Sequences and Binet-Fibonacci Curves. arXiv preprint arXiv:**1707.09151**.

[6] D. Saba .N.M, (Foundations of Mathematics), College of Ibn Al Haitham Of Science, University of Baghdad, Lectures Notes in Fund, 2010.

[7] Grimaldi, R. (2012). Fibonacci and Catalan Numbers: an introduction. John Wiley & Sons

[8] Johnson, R. C. (2009). Fibonacci numbers and matrices. Durham University.

[9] Ghosh, N. (2018). Fibonacci numbers in real life applications. *Mugberia Gangadhar Mahavidyalaya*, *1*, 62-69.

تقنية جديدة في التشفير باستخدام مصفوفات فايبوناشي ونظام Play-Fair

عوني محمد كفطان ، اكرم سالم محمد ، صلاح فلاح طرفة

قسم الرياضيات ، كلية علوم الحاسوب والرياضيات ، جامعة تكريت ، تكريت ، العراق

الملخص

في هذا البحث قدمنا تقنية جديدة تعتمد على على استخدام مصفوفات ومتتابعات فايبوناشي مع احدى طرق التشفير وهي طريقة Play-Fair هذه الطريقة يكون تطبيقها على خطوتين الأولى يتم فيها توليد مصفوفة مفتاحية بالاعتماد على خصائص سلسلة فايبوناشي للحصول على النص المشفر الأول وفي الخطوة الثانية نستخدم طريقة Play-Fair للحصول على النص المشفر الثاني (النهائي).