IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 12, Issue 2 Ver. II (Mar. - Apr. 2016), PP 66-72
www.iosrjournals.org

Multiple Encryptions of Fibonacci Lucas transformations

A. ChandraSekhar[1], Ch.Pragathi[2] , D.Chaya Kumari[3] and Ashok kumar[4]
[1]*Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India*
[2]*Associate Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India*
[3]*Assistant Professor in Mathematics, BVRIT Hyderabad College of engineering for women, Hyderabad, India*
[4]*Research Scholar, Department of Mathematics, GITAM University, Visakhapatnam, India*

Abstract: *Multiple encryptions in a practical system refers to encrypting the data more than once i.e., twice or trice to increase the security levels. As long as the cipher is unbreakable the encryption schemes remains strong. In view of the known attacks encrypting the data more than once will strengthen the security levels. In this paper we proposed a triple encryption scheme by using two keys generated by the mathematical structures from the number-theoretic concepts.*
Keywords: *Fibonacci numbers, Lucas numbers, Fibonacci-Lucas, Affine, Vignere transformations.*

I. Introduction

Multilevel encryption[1][10] is a process of encrypting the information which is encrypted one or more than once. Fibonacci Lucas numbers and Fibonacci Lucas matrices play a vital role in cryptography. We construct cryptosystem Fibonacci Lucas transformation. Fibonacci Lucas matrices are used as trapdoor function in public key cryptosystem.

1. Fibonacci Numbers

The Fibonacci sequence [3][7][13]is 1, 1, 2, 3, 5, 8. . . Where each entry is formed by adding the two previous ones, starting with 1 and 1 as the first two terms. This sequence is called Fibonacci sequence.

1.1 Properties of Fibonacci numbers

Fibonacci numbers are given by the following recurrence relation $F_{n+1} = F_n + F_{n-1}$ with the initial conditions $F_1 = F_2 = 1$

2. Lucas Number

The Lucas number [3][7][13] is defined to be the sum of its two immediate previous terms, thereby forming a Fibonacci integer sequence. The first two Lucas numbers are L_0 = 2 and L_1 = 1 as opposed to the first two Fibonacci numbers F_0 = 0 and F_1 = 1. Though closely related in definition, Lucas and Fibonacci numbers exhibit distinct properties. The Lucas numbers may thus be defined as follows:

$$L_n = \begin{cases} 2 & if\ n = 0 \\ 1 & if\ n = 1 \\ L_{n-1} + L_{n-2} & if\ n > 1 \end{cases}$$

The sequence of Lucas numbers is: 2,1,3,4,7,11,18,29,47,76,123,189…..

3. Fibonacci-Lucas Transform

The Fibonacci-Lucas Transformation[14] can be defined the mapping FL:$T^2 \rightarrow T^2$ such that $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} F_i & F_{i+1} \\ L_i & L_{i+1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\bmod N)$ Where x, y $\in \{0,1,2,......N-1\}$, F_i is the i^{st} term of Fibonacci series and L_i is the i^{st} term of Lucas series. Denoting $\begin{pmatrix} F_i & F_{i+1} \\ L_i & L_{i+1} \end{pmatrix}$. Continue in this way we can form an infinitely many transformations

Affine Cipher

An affine enciphering transformationis $C \equiv aP + b\left(\mathrm{mod}\, N\right)$ where the pair (a, b) is the encrypting key and gcd(a,N)=1. If y = E(x) = (ax+b)mod26,[1]then we can "solve for x in terms of y" and so $E^{-1}(y)$ that is, if $y \equiv (ax+b)\ \mathrm{mod}\, 26$ then $y - b \equiv ax(\mathrm{mod}\, 26)$ or equivalently $ax \equiv (y-b)\ \mathrm{mod}\, 26$

3.1 Vignere ciphere

The Vigenere cipher was generated by Giovan Batista Belaso in 1553[1]. This cipher uses a secret keyword to encrypt the plaintext. First, each letter in the plaintext is converted into a number. Then this numerical value for each letter of the plaintext is added to the numerical value of each letter of a secret keyword to get the ciphertext. The Vigenere ciphers are more powerful than substitution ciphers.

4. Proposed Work

An Algorithm for multi encryption using offset rule with Fibonacci numbers as the first layer of encryption and the affine transformation for super encryption

Multiple Encryption

Encryption algorithm:

Step-1: Alice creates plaintexts P = $p_1\ p_2,\ p_3 \ldots\ p_m$

Step-2: Alice computes C_1=P×(FL)and get 1st ciphertext

Step-3: Now Alice perform super encryption with C_1 to Affine transformation E(x) = (ax+b) mod 26, Gcd(a,N)=1 and for a and b are secrete, from the first level encryption message.

Step-4: Alice sends super encrypted message to Bob.

Decryption algorithm:

Step-1: Bob receives the super encrypted message.

Step-2: Bob decrypts the super encrypted message by using $E^{-1}\left(y\right) = a^{-1}\left(y - b\right)\mathrm{mod}\, 26$ (=P_1)

Step-3: Bob computes P=P_1×$(FL)^{-1}$ to get the original plaintext message.

Super Encyption of Vigenere Cipher

Encryption algorithm:

Step-1: Alice creates plaintexts P = $p_1\ p_2,\ p_3 \ldots\ldots\ p_m$

Step-2: Alice computes C_1=P×(FL) and get 1sr ciphertext and get 1st ciphertext

Step-3: Now Alice apply super encryption of vigenere transformation use off set rule with to the numerical value of each letter of a secret keyword to first level encryption message.

Step-4: Alice sends super encryption message to Bob.

Decryption algorithm:

Step-1: Bob receives the super encryption message.

Step-2: Bob use reverse off set rule with vigenere transformation to get first decrypted text P_1

Step-3: Bob computes P=P_1×$(\mathrm{FL})^{-1}$ to get the original plaintext message.

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 we get $FL = \begin{pmatrix} F_1 & F_2 \\ L_1 & L_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$

Encryption algorithm:

Step-1: Let the Plain text P= $\begin{pmatrix} H & A \\ C & K \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix}$

Step-2: Alice computes C_1= P×(FL)

$$\begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 7 \\ 22 & 12 \end{pmatrix}$$

Step-3: Now applying affine transformation E(x)=(ax+b) mod 26 for a = 5 & b= 25

x	7	7	22	12
5x+25	60	60	135	85
(5x+25)mod26	8	8	5	7
Second Encrypted message is	I	I	F	H

Step-4: Encrypted message is IIFH

Decryption algorithm:
Step-1: First Decrypted Message is IIFH
Step-2: Compute Inverse of Affine transformation $E^{-1}(y) = a^{-1}(y-b) \bmod 26$

Message	I	I	F	H
y	8	8	5	7
y-25	-17	-17	-20	-18
21(y-25)	-357	-357	-420	-378
21(y-25)mod26	7	7	22	12
First Decrypted text	H	H	W	M

$P_1 = \begin{pmatrix} H & H \\ W & M \end{pmatrix} = \begin{pmatrix} 7 & 7 \\ 22 & 12 \end{pmatrix}$

Step-3: Bob Compute $P_1 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 7 & 7 \\ 22 & 12 \end{pmatrix} \times \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix}$

	7	0	2	10
Mod 26	7	0	2	10
Second Decrypted message is	H	A	C	K

Case-2: For i=2 $FL = \begin{pmatrix} F_2 & F_3 \\ L_2 & L_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$

Encryption algorithm:

Step-1: Let the Plain text P= $\begin{pmatrix} H & A \\ C & K \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix}$

Step-2: Alice computes $C_1 = P \times (FL)$

$\begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 7 & 14 \\ 12 & 34 \end{pmatrix}$

Step-3: Now applying affine transformation E(x)=(ax+b) mod 26 for a = 5 & b= 30

x	7	14	12	34
5x+30	65	100	90	200
(5x+30)mod26	13	22	12	8
Second Encrypted message is	N	W	M	S

Step-4: Encrypted message is NWMS

Decryption algorithm:
Step-1: First Decrypted Message is NWMS
Step-2: Compute Inverse of Affine transformation $E^{-1}(y) = a^{-1}(y-b) \bmod 26$

Message	N	W	M	S
x	13	22	12	18
y-30	-17	-8	-18	-12
21(y-30)	-357	-168	-378	-252
21(y-30)mod26	7	14	12	8
First Decrypted text	H	O	M	I

P_1= $\begin{pmatrix} H & O \\ M & I \end{pmatrix} = \begin{pmatrix} 7 & 14 \\ 12 & 8 \end{pmatrix}$

Step-3: Bob Compute $P_1 \times (FL)^{-1}$ to get original message P now $\begin{pmatrix} 7 & 14 \\ 12 & 8 \end{pmatrix} \times \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 28 & -16 \end{pmatrix}$

	7	0	28	-16
Mod 26	7	0	2	10
Second Decrypted message is	H	A	C	K

Case-3: For i=3 $FL = \begin{pmatrix} F_3 & F_4 \\ L_3 & L_4 \end{pmatrix}$ = $\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$

Encryption algorithm:

Step-1: Let the Plain text P= $\begin{pmatrix} H & A \\ C & K \end{pmatrix}$ = $\begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix}$

Step-2: Alice computes C_1= P×(FL)

$\begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 14 & 21 \\ 34 & 46 \end{pmatrix}$

Step-3: Now applying affine transformation E(x)=(ax+b) mod 26 for a = 5 & b= 29

x	14	21	34	46
5x+29	99	134	199	259
(5x+29)mod26	21	4	17	25
Second Encrypted message is	V	E	R	Z

Step-4: Encrypted message is VERZ

Decryption algorithm:

Step-1: First Decrypted Message is VERZ

Step-2: Compute Inverse of Affine transformation $E^{-1}(y) = a^{-1}(y-b) \bmod 26$

Message	V	E	R	Z
y	21	4	17	25
y-29	-8	-25	-12	-4
21(y-29)	-168	-525	-252	-84
21(y-29)mod26	14	21	8	20
First Decrypted text	O	V	I	U

P_1= $\begin{pmatrix} O & V \\ I & U \end{pmatrix} = \begin{pmatrix} 14 & 21 \\ 8 & 20 \end{pmatrix}$

Step-3: Bob Compute P_1×$(FL)^{-1}$ to get original message P

now $\begin{pmatrix} 14 & 21 \\ 8 & 20 \end{pmatrix} \times \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 28 & -16 \end{pmatrix}$

	7	0	28	-16
Mod 26	7	0	2	10
Second Decrypted message is	H	A	C	K

Vigenere Cipher

Case:1 For i=1 we get $FL = \begin{pmatrix} F_1 & F_2 \\ L_1 & L_2 \end{pmatrix}$ = $\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$

Encryption algorithm:

Step-1: Let the Plain text P = $\begin{pmatrix} R & A \\ M & U \end{pmatrix}$ = $\begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix}$

Step-2: Alice computes C_1= P×(FL)

$\begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 17 & 17 \\ 52 & 32 \end{pmatrix}$

Using vigenere ciphers for key

P	A	S	S

15	0	18	18

Step-3: Offset rule with the first decrypted message

	17	17	52	32
Offset rule with key	17 + 15	17 + 0	32 + 18	12 + 18
	32	17	70	50
Mod 26	6	17	18	24
Second Encrypted message is	G	R	S	Y

Step-4: Encrypted message is GRSY

Decryption algorithm:

Step-1: First Decrypted Message is GRSY

Step-2: Bob use reverse off set rule with vigenere transformation to get first decrypted text.

Message	G	R	S	Y
	6	17	18	24
Reverse offset rule with key	6 - 15	17 - 0	18 - 18	24 - 18
	-9	17	0	6
Mod 26	17	17	0	6
First Decryption message is	**R**	**R**	**A**	**G**

P_1= $\begin{pmatrix} R & R \\ A & G \end{pmatrix} = \begin{pmatrix} 17 & 17 \\ 0 & 6 \end{pmatrix}$

Step-3: Bob Compute $P_1 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 17 & 17 \\ 0 & 6 \end{pmatrix} \times \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 17 & 0 \\ 12 & -6 \end{pmatrix}$

	17	0	12	-6
Mod 26	17	0	12	20
Second Decrypted message is	R	A	M	U

Case-2: For i=2 $FL = \begin{pmatrix} F_2 & F_3 \\ L_2 & L_3 \end{pmatrix}$ **=** $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$

Encryption algorithm:

Step-1: Let the Plain text P = $\begin{pmatrix} R & A \\ M & U \end{pmatrix}$ **=** $\begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix}$

Step-2: Alice computes C_1= P×(FL)

$\begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 17 & 34 \\ 32 & 84 \end{pmatrix}$

Using vigenere ciphers for key

F	A	I	L
5	0	8	11

Step-3: Offset rule with the first decrypted message

	17	34	32	84
Offset rule with key	17 + 5	34 + 0	42 + 8	84 + 11
	22	34	50	95
Mod 26	22	8	24	17
Second Encrypted message is	W	I	Y	R

Step-4: Encrypted message is WIYR

Decryption algorithm:

Step-1: First Decrypted Message is WIYR

Step-2: Bob use reverse off set rule with vigenere transformation to get first decrypted text.

Message	W	I	Y	R
	22	8	24	17
Reverse offset rule with key	22 - 5	8 - 0	24 - 8	17 - 11
	-9	8	6	6
Mod 26	17	8	6	6
First Decryption message is	I	R	S	G

P_1= $\begin{pmatrix} R & I \\ G & G \end{pmatrix} = \begin{pmatrix} 17 & 8 \\ 6 & 6 \end{pmatrix}$

Step-3: Bob Compute $P_1 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 17 & 8 \\ 6 & 6 \end{pmatrix} \times \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 43 & -26 \\ 12 & -6 \end{pmatrix}$

	43	-26	12	-6
Mod 26	17	0	12	20
Second Decrypted message is	R	A	M	U

Case-3: For i=3 $FL = \begin{pmatrix} F_3 & F_4 \\ L_3 & L_4 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$

Encryption algorithm:

Step-1: Let the Plain text P = $\begin{pmatrix} R & A \\ M & U \end{pmatrix} = \begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix}$

Step-2: Alice computes C_1= P×(FL)

$\begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 34 & 51 \\ 84 & 116 \end{pmatrix}$

Using vigenere cipher for the key

L	O	S	S
11	14	18	18

Step-3: Offset rule with the first decrypted message

	34	51	84	116
Offset rule with key	34 + 11	51 + 14	84 + 18	116 + 18
	45	65	102	134
Mod 26	19	13	24	4
Second Encrypted message is	T	N	Y	E

Step-4: Encrypted message is TNYE

Decryption algorithm:

Step-1: First Decrypted Message is TNYE

Step-2: Bob use reverse off set rule with vigenere transformation to get first decrypted text.

Message	T	N	Y	E
	19	13	24	4
Reverse offset rule with key	19 - 11	13 - 14	24 - 18	4 - 18
	8	-1	6	-14
Mod 26	8	25	6	12
First Decryption message is	I	Z	G	M

P_1 = $\begin{pmatrix} I & Z \\ G & M \end{pmatrix} = \begin{pmatrix} 8 & 25 \\ 6 & 12 \end{pmatrix}$

Step-3: Bob Compute $P_1 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 8 & 25 \\ 6 & 12 \end{pmatrix} \times \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 43 & -26 \\ 12 & -6 \end{pmatrix}$

	43	-26	12	-6
Mod 26	17	0	12	20
Second Decrypted message is	R	A	M	U

II. Conclusions

For this constructed cryptosystem the time complexity for encryption and decryption are same but is more secure than the symmetric cryptosystems with Fibonacci, Lucas, Pell numbers we can exiled this concept to public key cryptosystem also.

References

[1] A. ChandraSekhar, D. Chaya Kumari, S. Ashok Kumar "Symmetric Key Cryptosystem for Multiple Encryptions",*International Journal of Mathematics Trends and Technology (IJMTT).* V29 (2):140-144 January 2016. ISSN:2231-5373.

[1] A. Chandra Sekhar, Prasad Reddy. P.V.G.D, A.S.N.Murty, B.Krishna Gandhi "Self-Encrypting Data Streams Using Graph Structures" IETECH International Journal Of Advanced Computations PP 007-009, 2008, vol 2.

[2] A.P.Stakhov " The Golden matrices and a new kind of cryptography" chaos, solutions and Fractals 32(2007) pp1138-1146.

[3] A.P.Stakhov " The Golden section and modern harmony mathematics. Applications of Fibonacci numbers" ,kluwer Academic publishers (1998). pp393-399

[4] A. Chandra Sekhar, K.R. Sudha and Prasad Reddy. P.V.G.D "Data Encryption Technique Using Random Generator" IEEE International Conference on Granular Computing GrC-07, Nov 2-4, 2007, Silicon Valley, USA, PP 576-579.

[5] B.Krishna Gandhi, A. Chandra Sekhar and Prasad Reddy P.V.G.D: Cryptographic Scheme for Digital signals" INTECH International Journal Of Advanced Computations", Vol:2 No:4, PP195-200,2008.

[6] "E.H.Lock Wood, A single-light on pascal's triangle, Math, Gazette 51(1967), PP 243-244.

[7] Fibonacci, Lucas and Pell numbers andpascal's triangle, Thomas Khoshy, Applied Probability Trust, PP 125-132.

[8] Fibonacci and lucas numbers with applications thomas Khoshy ISBN: 978-0-471-39939-8.

[9] K.R.Sudha, A. Chandra Sekhar, P.V.G.D, Prasad Reddy, "Cryptographic Protection Of Digital Signal Using some Recurrence Relations" IJCNS, May 2007, PP203-207.

[10] Linear independent spanning sets and linear transformations for multi-level encryption, A.ChandraSekhar, V.Anusha, B.Ravi Kumar, S.Ashok Kumar Vol36(2015) , No.4, PP;385-392.

[11] Tianping Zhang, Yuankui Ma" On Generalized Fibonacci Polynomials and Bernouli Numbers" Journal of Integer sequence, Vol.8 (2005),PP 1-6

[12] T.Koshy, Fibonacci and Lucas Numbers with applications, John Wiley and Sons,NY,2001.

[13] Hoggat VE."Fibonacci and Lucas numbers" palo Alto,CA:Houghton-Mifflin;1969.

[14] International journal on cryptography and information security(IJCI") "Image encryption using Fibonacci-Lucas transformation" Vol.2,No3,September 2012.