Available online at http://www.journalijdr.com

International Journal of
DEVELOPMENT RESEARCH

ISSN: 2230-9926

International Journal of Development Research
Vol. 6, Issue, 03, pp. 7079-7089, March, 2016

Full Length Research Article

TRIPLE ENCRYPTION OF MULTIPLE KEYS FOR SYMMETRIC KEY CRYPTO SYSTEMS

[1]ChandraSekhar, A., [2]Ch.Pragathi and [3,*]Ashok Kumar

[1]Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India
[2]Associate Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India
[3]Research Scholar, Department of Mathematics, GITAM University, Visakhapatnam, India

ARTICLE INFO

Article History:

Received 19th December, 2015
Received in revised form
08th January, 2016
Accepted 24th February, 2016
Published online 31st March, 2016

Key Words:

Fibonacci numbers,
Lucas numbers Affine,
Vignere,
Fibonacci-Lucas Transformations.

ABSTRACT

Multiple encryptions in a practical system refers to encrypting the data more than once i.e., encrypting the data 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.

INTRODUCTION

Multilevel encryption 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.

Fibonacci Numbers

The Fibonacci sequence 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.

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 $F_1 = F_2 = 1$

Lucas Number

The Lucas number 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:

***Corresponding author: Ashok Kumar,**
Research Scholar, Department of Mathematics, GITAM University, Visakhapatnam, India.

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

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

Pell Numbers

The Pell numbers are defined by the recurrence relation

$$P_n = \begin{cases} 0 & if\ n = 0 \\ 1 & if\ n = 1 \\ 2P_{n-1} + P_{n-2} & other\ wise \end{cases}$$

In words, the sequence of Pell numbers starts with 0 and 1, and then each Pell number is the sum of twice the previous Pell number and the Pell number before that. The first few terms of the sequence are 0,1,2,5,12,29,70,169, 408,985, 2378, 5741, 13890,...

Fibonacci-Lucas Transform

The Fibonacci-Lucas Transformation 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[th] term of Fibonacci series and L_i is the i[th] 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 $C \equiv aP + b(\bmod N)$ where the pair (a, b) is the encrypting key and gcd (a,N)=1. If y = E(x) = (ax+b) mod 26, [1] then we can "solve for x in terms of y" and so $E^{-1}(y)$ that is, if $y \equiv (ax+b) \bmod 26$ then $y - b \equiv ax(\bmod 26)$ or equivalently $ax \equiv (y-b) \bmod 26$

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.

Proposed Work

An Algorithm for triple encryption using offs Fibonacci-Lucas transformation as the first layer of encryption, decrypting with the inverse of the Affine transformation as the second layer of encryption and finally encrypting with the Fibonacci- Lucas transformation as the third layer of 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 1[sr] ciphertext
Step-3: Alice decrypts the super encrypted message by using $E^{-1}(y) = a^{-1}(y-b) \bmod 26$ (=C_2)
Step-4: Alice computes C_2×(FL)=C_3
Step-5: Alice sends message C_3 to Bob.
Decryption algorithm:
Step-1: Bob receives the encrypted message C_3.
Step-2: Bob compute $C_3 \times (FL)^{-1} = P_2$

Step-3: Now Bob compute P_1 decrypted with the 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: Bob computes $P=P_1\times(FL)^{-1}$ to get the original plaintext message P.

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

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= $\begin{pmatrix} T & E \\ X & T \end{pmatrix}=\begin{pmatrix} 19 & 4 \\ 23 & 19 \end{pmatrix}$

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

$$\begin{pmatrix} 19 & 4 \\ 23 & 19 \end{pmatrix}\times\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}=\begin{pmatrix} 27 & 23 \\ 61 & 42 \end{pmatrix}$$

	27	23	61	42
Mod 26	1	23	9	16

$$C_1=\begin{pmatrix} 1 & 23 \\ 9 & 16 \end{pmatrix}$$

Step-3: Alice Compute Inverse of Affine transformation $E^{-1}(y)=a^{-1}(y-b)\bmod 26$ for a = 5 & b= 16

y	1	23	9	16
y-16	-15	7	-7	0
21(y-16)	-315	147	-147	0
21(y-16) mod 26	23	17	9	0

$C_2 = \begin{pmatrix} 23 & 17 \\ 9 & 0 \end{pmatrix}$

Step-4: Alice computes $C_2\times(FL)=C_3$

$$\begin{pmatrix} 23 & 17 \\ 9 & 0 \end{pmatrix}\times\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}=\begin{pmatrix} 57 & 40 \\ 9 & 9 \end{pmatrix}$$

	57	40	9	9
Mod 26	5	14	9	9

Step-4: Encrypted message C_3 is FOJJ

Decryption algorithm

Step-1: First Decrypted Message is FOJJ

Step-2: Bob compute $C_3 \times (FL)^{-1}=P_2$

$$\begin{pmatrix} 5 & 14 \\ 9 & 9 \end{pmatrix}\times\begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix}=\begin{pmatrix} 23 & -9 \\ 9 & 0 \end{pmatrix}$$

	23	-9	9	0
Mod 26	23	17	9	0

$$P_2 = \begin{pmatrix} 23 & 17 \\ 9 & 0 \end{pmatrix}$$

Step-3: Now applying affine transformation E(x)=(ax+b) mod 26 for a = 5 & b= 16

x	23	17	9	0
5x+16	131	101	61	16
(5x+16)mod26	1	23	9	16
Decrypted message is	B	X	J	Q

$$P_1 = \begin{pmatrix} 1 & 23 \\ 9 & 16 \end{pmatrix}$$

Step-4: Bob Compute $P_1 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 1 & 23 \\ 9 & 16 \end{pmatrix} \times \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 45 & -22 \\ 23 & -7 \end{pmatrix}$

	45	-22	23	-7
Mod 26	19	4	23	19
Second Decrypted message is	**T**	E	X	T

Case-2: For i= 2we get $FL = \begin{pmatrix} F_1 & F_2 \\ L_1 & L_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$

Encryption algorithm

Step-1: Let the Plain text P= $\begin{pmatrix} T & E \\ X & T \end{pmatrix} = \begin{pmatrix} 19 & 4 \\ 23 & 19 \end{pmatrix}$

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

$$\begin{pmatrix} 19 & 4 \\ 23 & 19 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 23 & 50 \\ 42 & 103 \end{pmatrix}$$

	23	50	42	103
Mod 26	23	24	16	25

$$C_1 = \begin{pmatrix} 23 & 24 \\ 16 & 25 \end{pmatrix}$$

Step-3: Alice Compute Inverse of Affine transformation $E^{-1}(y) = a^{-1}(y-b) \bmod 26$ for a = 5 & b= 18

y	23	24	16	25
y-18	5	6	-2	7
21(y-18)	105	126	-42	147
21(y-18) mod 26	1	22	10	17

$$C_2 = \begin{pmatrix} 1 & 22 \\ 10 & 17 \end{pmatrix}$$

Step-4: Alice computes $C_2 \times (FL) = C_3$

$$\begin{pmatrix} 1 & 22 \\ 10 & 17 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 23 & 68 \\ 27 & 71 \end{pmatrix}$$

	23	68	27	71
Mod 26	23	16	1	19

Step-4: Encrypted message C_3 is XQBT

Decryption algorithm

Step-1: First Decrypted Message is XQBT

Step-2: Bob compute $C_3 \times (FL)^{-1} = P_2$

$$\begin{pmatrix} 23 & 16 \\ 1 & 19 \end{pmatrix} \times \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 53 & -30 \\ -16 & 17 \end{pmatrix}$$

	53	-30	-16	17
Mod 26	1	22	10	17

$$P_2 = \begin{pmatrix} 1 & 22 \\ 10 & 17 \end{pmatrix}$$

Step-3: Now applying affine transformation E(x)=(ax+b) mod 26 for a = 5 & b= 18

x	1	22	10	17
5x+18	23	128	68	103
(5x+18)mod26	23	24	16	25
Decrypted message is	X	Y	Q	Z

$$P_1 = \begin{pmatrix} 23 & 24 \\ 16 & 25 \end{pmatrix}$$

Step-4: Bob Compute $P_1 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 23 & 24 \\ 16 & 25 \end{pmatrix} \times \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 45 & -22 \\ 23 & -7 \end{pmatrix}$

	45	-22	23	-7
Mod 26	19	4	23	19
Second Decrypted message is	T	E	X	T

Case-3: For i=3 we get $FL = \begin{pmatrix} F_1 & F_2 \\ L_1 & L_2 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$

Encryption algorithm:

Step-1: Let the Plain text P= $\begin{pmatrix} T & E \\ X & T \end{pmatrix} = \begin{pmatrix} 19 & 4 \\ 23 & 19 \end{pmatrix}$

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

$$\begin{pmatrix} 19 & 4 \\ 23 & 19 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 50 & 73 \\ 103 & 145 \end{pmatrix}$$

	50	73	103	145
Mod 26	24	21	25	15

$$C_1 = \begin{pmatrix} 24 & 21 \\ 25 & 15 \end{pmatrix}$$

Step-3: Alice Compute Inverse of Affine transformation $E^{-1}(y) = a^{-1}(y-b) \bmod 26$ for a = 5 & b= 21

y	24	21	25	15
y-21	3	0	4	-6
21(y-21)	63	0	84	-126
21(y-21) mod 26	11	0	6	4

$$C_2 = \begin{pmatrix} 11 & 0 \\ 6 & 4 \end{pmatrix}$$

Step-4: Alice computes $C_2 \times (FL) = C_3$

$$\begin{pmatrix} 11 & 0 \\ 6 & 4 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 22 & 33 \\ 24 & 34 \end{pmatrix}$$

	22	33	24	34
Mod 26	22	7	24	8

Step-4: Encrypted message C_3 is WHYI

Decryption algorithm

Step-1: First Decrypted Message is WHYI

Step-2: Bob compute $C_3 \times (FL)^{-1} = P_2$

$$\begin{pmatrix} 22 & 7 \\ 24 & 8 \end{pmatrix} \times \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} -67 & 52 \\ -72 & 56 \end{pmatrix}$$

	-67	52	-72	56
Mod 26	11	0	6	4

$$P_2 = \begin{pmatrix} 11 & 0 \\ 6 & 4 \end{pmatrix}$$

Step-3: Now applying affine transformation E(x)=(ax+b) mod 26 for a = 5 & b= 21

x	11	0	6	4
5x+21	76	21	51	41
(5x+21)mod26	24	21	24	15
Decrypted message is	Y	V	Y	P

$$P_1 = \begin{pmatrix} 24 & 21 \\ 24 & 15 \end{pmatrix}$$

Step-4: Bob Compute $P_1 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 24 & 21 \\ 25 & 15 \end{pmatrix} \times \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} -33 & 30 \\ -55 & 45 \end{pmatrix}$

	-33	30	-55	45
Mod 26	19	4	23	19
Second Decrypted message is	T	E	X	T

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 = $\begin{pmatrix} G & O \\ L & D \end{pmatrix} = \begin{pmatrix} 6 & 14 \\ 11 & 3 \end{pmatrix}$

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

$$\begin{pmatrix} 6 & 14 \\ 11 & 3 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 34 & 20 \\ 17 & 14 \end{pmatrix}$$

$$C_1 = \begin{pmatrix} 34 & 20 \\ 17 & 14 \end{pmatrix}$$

Using vigenere ciphers for key

L	O	V	E
11	14	21	4

Step-3: Alice compute reverse offset rule with the first encrypted message C_1

	34	20	17	14
Reverse offset rule with key	34 - 11	20 - 14	17 - 21	14 - 4
	23	6	-4	10
Mod 26	23	6	22	10
Second Encrypted message is	X	G	W	K

Second Encrypted message is $C_2 = \begin{pmatrix} 23 & 6 \\ 22 & 10 \end{pmatrix}$

Step-4: Alice compute $C_2\times(FL)=C_3$

$$\begin{pmatrix} 23 & 6 \\ 22 & 10 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 35 & 29 \\ 42 & 32 \end{pmatrix}$$

	35	29	42	32
Mod 26	9	3	16	6
Third encrypted message is	J	D	Q	H

Step-5: Alice send message C_3 to bob JDQH

Decryption algorithm

Step-1: First Decrypted Message is JDQH

Step-2: Bob compute $C_3 \times (FL)^{-1} = P_2$

$$\begin{pmatrix} 9 & 3 \\ 16 & 6 \end{pmatrix} \times \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} -3 & 6 \\ -4 & 10 \end{pmatrix}$$

Step-2: Bob Decrypts with the offset rule with vigenere transformation

	-3	6	-4	10
Offset rule with key	-3 + 11	6 + 14	-4 + 21	10 + 4
	8	20	17	14
Mod 26	8	20	17	14
Second Decryption message is	I	U	R	O

$$\mathbf{P_2}=\begin{pmatrix} I & U \\ R & O \end{pmatrix}$$

Step-3: Bob Compute $P_2 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 8 & 20 \\ 17 & 14 \end{pmatrix} \times \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 32 & -12 \\ 11 & 3 \end{pmatrix}$

	32	-12	11	3
Mod 26	6	14	11	3
Third Decrypted message is	G	O	L	D

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 = $\begin{pmatrix} N & E \\ W & S \end{pmatrix} = \begin{pmatrix} 13 & 4 \\ 22 & 18 \end{pmatrix}$

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

$$\begin{pmatrix} 13 & 4 \\ 22 & 18 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 17 & 38 \\ 40 & 98 \end{pmatrix}$$

$C_1 = \begin{pmatrix} 17 & 38 \\ 40 & 98 \end{pmatrix}$

Using vigenere ciphers for key

L	O	V	E
11	14	21	4

Step-3: Alice compute reverse offset rule with the first encrypted message C_1

	17	38	40	98
Reverse offset rule with key	17 - 11	38 - 14	40 - 21	98 - 4
	6	24	19	94
Mod 26	6	24	19	16
Second Encrypted message is	G	Y	T	Q

Second Encrypted message is $C_2 = \begin{pmatrix} 6 & 24 \\ 19 & 16 \end{pmatrix}$

Step-4: Alice compute $C_2 \times (FL) = C_3$

$$\begin{pmatrix} 6 & 24 \\ 19 & 16 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 30 & 84 \\ 35 & 86 \end{pmatrix}$$

	30	84	35	86
Mod 26	4	6	9	8
Third encrypted message is	E	G	J	I

Step-5: Alice send message C_3 to bob EGJI

Decryption algorithm

Step-1: First Decrypted Message is EGJI

Step-2: Bob compute $C_3 \times (FL)^{-1} = P_2$

$$\begin{pmatrix} 4 & 6 \\ 9 & 8 \end{pmatrix} \times \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 6 & -2 \\ 19 & -10 \end{pmatrix}$$

Step-2: Bob Decrypts with the offset rule with vigenere transformation

	6	-2	19	-10
Offset rule with key	6 + 11	-2 + 14	19 + 21	-10 + 4
	17	38	40	20
Mod 26	17	12	14	20
Second Decryption message is	**R**	**M**	**O**	**U**

$$\mathbf{P_2} = \begin{pmatrix} R & M \\ O & U \end{pmatrix}$$

Step-3: Bob Compute $P_2 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 17 & 12 \\ 14 & 20 \end{pmatrix} \times \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 39 & -22 \\ 22 & -8 \end{pmatrix}$

	39	-22	22	-8
Mod 26	13	4	22	18
Third Decrypted message is	N	E	W	S

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 = $\begin{pmatrix} T & E \\ C & H \end{pmatrix} = \begin{pmatrix} 19 & 4 \\ 2 & 7 \end{pmatrix}$

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

$$\begin{pmatrix} 19 & 4 \\ 2 & 7 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 50 & 73 \\ 25 & 34 \end{pmatrix}$$

$C_1 = \begin{pmatrix} 50 & 73 \\ 25 & 34 \end{pmatrix}$

Using vigenere ciphers for key

L	O	V	E
11	14	21	4

Step-3: Alice compute reverse offset rule with the first encrypted message C_1

	50	73	25	34
	50	73	25	34

Reverse offset rule with key	- 11	- 14	- 21	- 4
	39	59	4	30
Mod 26	13	7	4	4
Second Encrypted message is	N	H	E	E

Second Encrypted message is $C_2 = \begin{pmatrix} 13 & 7 \\ 4 & 4 \end{pmatrix}$

Step-4: Alice compute $C_2 \times (FL) = C_3$

$$\begin{pmatrix} 13 & 7 \\ 4 & 4 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 47 & 67 \\ 20 & 28 \end{pmatrix}$$

	47	67	20	28
Mod 26	21	15	20	2
Third encrypted message is	V	P	U	C

Step-5: Alice send message C_3 to bob VPUC

Decryption algorithm

Step-1: First Decrypted Message is VPUC

Step-2: Bob compute $C_3 \times (FL)^{-1} = P_2$

$$\begin{pmatrix} 21 & 15 \\ 20 & 2 \end{pmatrix} \times \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} -39 & 33 \\ -74 & 56 \end{pmatrix}$$

Step-2: Bob Decrypts with the offset rule with vigenere transformation

	-39	33	-74	56
Offset rule with key	-39 + 11	33 + 14	-74 + 21	56 + 4
	-28	47	-53	60
Mod 26	24	21	25	8
Second Decryption message is	**Y**	**V**	**Z**	**I**

$$\mathbf{P_2} = \begin{pmatrix} Y & V \\ Z & I \end{pmatrix}$$

Step-3: Bob Compute $P_2 \times (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 24 & 21 \\ 25 & 8 \end{pmatrix} \times \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} -33 & 30 \\ -76 & 59 \end{pmatrix}$

	-33	30	-76	59
Mod 26	19	4	2	7
Third Decrypted message is	T	E	C	H

Conclusions

In the proposed technique only two keys were employed for triple encryption instead of using three keys for three layers of encryption. Time complexity is less for encryption by this method than the original triple encryption method.

REFERENCES

Branstad, D.K., Gait,J. and Katzke, S. 1976. Report of the workshop on cryptography in support of computer security, National Bureau of Standards Rep.NBSIR 77-1291(Sept.21-22).

Chandra Sekhar, A., Ch.prgathi, B. Ravi Kumar, S. and Ashok kumar 2016. “Multiple encryption of various ciphers” International Journal od Engineering Science Invention Research & Development; Vol.II Issue VIII February.

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

Diffie,W. and Hellman, M. 1977. Exhaustive cryptanalysis of the NBS data encryption Standard. Computer (June),74-84.

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

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

Hellman, M.E. 1977. An extension of the Shannon theory approach to cryptography,IEEE Trans.Info.IT-23, (May),289-294.

Hoggat, V.E. 1969. ”Fibonacci and Lucas numbers” palo Alto,CA:Houghton-Mifflin.

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

Kolata, G.B 1977. Computer encryption and the national security agency,Science 1977(July 29,)438-440.

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

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.

Lock Wood, E.H. 1967. A single-light on pascal's triangle, Math, Gazette 51, PP 243-244.

On the security of multiple encryption, Ralphe.merle, Elxs, Inti Martin E.Hellmon Standford University, Communication of the ACM July 1981, Vol 24 No 7.

Shannon,C.E. 1949. Communication theory of security systems.Bell. syst.Tech.J.28(OCT.),656-715.

Stakhov, A.P. 1998. “The Golden section and modern harmony mathematics. Applications of Fibonacci numbers” ,kluwer Academic publishers. pp393-399.

Stakhov, A.P. 2007 .“ The Golden matrices and a new kind of cryptography” chaos, solutions and Fractals 32 pp1138-1146.

Tianping Zhang, Yuankui Ma” 2005. On Generalized Fibonacci Polynomials and Bernouli Numbers” Journal of Integer sequence, Vol.8,PP 1-6

Tuchman,W.L. 1978. Talik presented at the Nat.Computer conf.,Anaheim,C.A.,June.

****