International Journal of Mathematical Archive-7(2), 2016, 103-110
Available online through www.ijma.info ISSN 2229 – 5046

MULTIPLE ENCRYPTIONS OF INDEPENDENT CIPHERS

A. CHANDRASEKHAR[1], D. CHAYA KUMARI*[2], CH.PRAGATHI[3] AND ASHOK KUMAR[4]

[1]Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India.

**[2]Assistant Professor in Mathematics,
BVRIT Hyderabad College of engineering for women, Hyderabad, India.**

[3]Associate Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India.

[4]Research Scholar, Department of Mathematics, GITAM University, Visakhapatnam, India.

(Received On: 12-02-16; Revised & Accepted On: 29-02-16)

ABSTRACT

T*he main aim of Cryptography is to protect user privacy. The modern ciphers which were employed in wireless networks, digital content and financial systems are rarely get cracked. In order to enhance the security levels, recent research work suggests multiple encryptions. For these issues designing of mathematical models from Algebraic Structures, Number Theoretic concepts play a vital role. In this paper we proposed multiple encryptions using Lucas, Pell numbers, Affine and Vigenere transformations as layers of encryption.*

Keywords: *Pell number, Lucas numbers, Affine, Vignere transformations,encryption algorithms, decryption algorithms.*

INTRODUCTION

Super-encryption is a process of encrypting the information that is already encrypted [5][13]. Multiple encryptions is the process of employing multiple ciphers. The generation of key for each cipher plays the pivotal role. Designing an algorithm for each layer of encryption requires independency. If one depends on the other then security levels are very low. Designing of mathematical models for multiple encryptions mostly based on time and space complexity.

Lucas Numbers

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:

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

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

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

Corresponding Author: D. Chaya Kumari[2], [2]Assistant Professor in Mathematics,
BVRIT Hyderabad College of engineering for women, Hyderabad, India.*

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,...

Affine Transformation

An affine enciphering transformation is $C \equiv aP + b \pmod N$ where the pair (a, b) is the encrypting key and gcd(a,N)=1. If y = E(x) = (ax+b) mod26,[5]then we can "solve for x in terms of y" and so $E^{-1}(y)$ that is, if $y \equiv (ax + b) \mod 26$ then $y - b \equiv ax \pmod{26}$ or equivalently $ax \equiv (y - b) \mod 26$.

Vigenere Transformation

The Vigenere cipher was generated by Giovan Batista Belaso in 1553[9]. 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.

Super encryption

Super-encryption is a process of encryption information that is already encrypted. Super encryption is simply the use of multiple ciphers, usually in multiple steps, as a singular encryption scheme and is a very important technique and many modern strong encryption algorithms can be regarded as resulting from super-encryption using a number of comparatively weak algorithm.

Present 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 with Lucas numbers

Encryption algorithm:

Step-1: Alice creates plaintexts P = p_1 p_2, p_3 ... p_m

Step-2: Alice use off set rule with Lucas numbers F=f_1, f_2, f_3... f_n to each value in sequential order and get 1^{sr} ciphertext

Step-3: Alice computes $C_i=P_i+F_i$ for i=1,2,3,…m where C_{1i} is the first construct cipher text.

Step-4: Now Alice perform super encryption with the Affine transformation E(x) = (ax+b) mod 26, Gcd(a, N)=1 and take a and b are secret, from the first level encryption message.

Step-5: 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 $E^{-1}(y) = a^{-1}(y - b) \mod 26$

Step-3: Using reverse offset rule with Lucas number Bob decrypts first decrypted message to get original plaintext.

SUPER ENCRYPTION OF VIGENERE CIPHER

Encryption algorithm:

Step-1: Alice creates plaintexts P = p_1 p_2, p_3..... p_m

Step-2: Alice use off set rule with Lucas numbers F=f_1 f_2 f_3... f_n to each value in sequential order and get 1^{sr} ciphertext

© 2016, IJMA. All Rights Reserved

Step-3: Alice computes $C_i=P_i+F_i$ for i=1, 2, 3,…m where C_{1i} is the first constructed cipher text.

Step-4: Alice super encrypts the first encrypted message with vigenere transformation using a secret key.

Step-5: Alice sends super encrypted message to Bob.

Decryption algorithm:

Step-1: Bob receives the super encrypted message.

Step-2: Bob decrypts with reverse offset rule vigenere transformation to super encryption message. It is the first decryption message

Step-3: Using reverse offset rule with Lucas number Bob decrypts first decrypted message to get original plaintext.

Multiple Encryption with Pell numbers

Encryption algorithm:

Step-1: Alice creates plaintexts P = p_1, p_2, p_3 ... p_m

Step-2: Alice use off set rule with Pell numbers F=f_1, f_2, f_3... f_n to each value in sequential order and get 1^{sr} cipher text

Step-3: Alice computes $C_i=P_i+F_i$ for i=1, 2, 3,…m where C_{1i} is the first construct cipher text.

Step-4: Now Alice apply super encryption of Affine transformation E(x) = (ax+b) mod 26, gcd(a, N) = 1 and take a and b are secret, from the first level encryption message.

Step-5: Alice sends super encrypted message to Bob.

Decryption algorithm:

Step-1: Bob receives the super encrypted message.

Step-2: Bob decrypts with the inverse affine transformation by using $E^{-1}(y)=a^{-1}(y-b)\bmod 26$ as super encrypted message. It is the first decryption message

Step-3: Using reverse offset rule with Pell number Bob decrypts first decrypted message to get original plaintext.

SUPER ENCRYPTION OF VIGENERE CIPHER

Encryption algorithm:

Step-1: Alice creates plaintexts P = p_1 p_2, p_3 ... p_m

Step-2: Alice use off set rule with Pell numbers F=f_1, f_2, f_3... f_n to each value in sequential order and get 1^{sr} ciphertext

Step-3: Alice computes $C_i=P_i+F_i$ for i=1,2,3,…m where C_{1i} is the first construct cipher text.

Step-4: Alice super encrypts the first encrypted message with vigenere transformation using a secret key

Step-5: Alice sends super encrypted message to Bob.

Decryption algorithm:

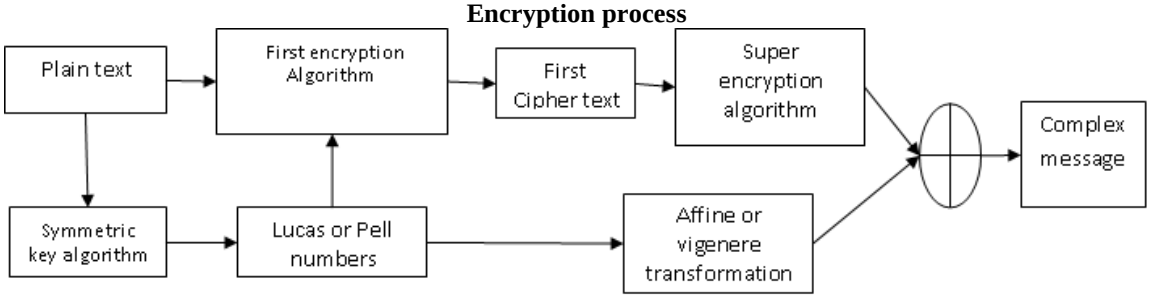
Step-1: Bob receives the super encrypted message.

Step-2: Bob decrypts with the reverse off set rule of vigenere transformation to super encryption message. It is the first decryption message

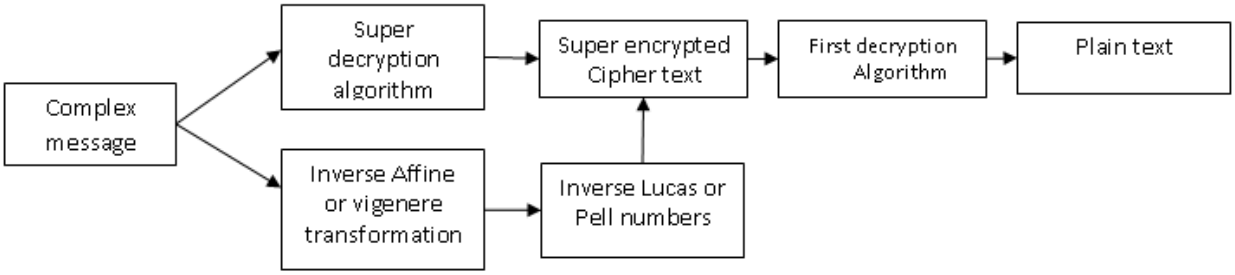
Step-3: Using reverse offset rule with Pell number Bob decrypts first decrypted message to get original plaintext.

© 2016, IJMA. All Rights Reserved

Encryption process



Decryption process



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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

EXAMPLE

Encryption algorithm:

Step-1: Let the Plain text be NUMBERTHEORY

Step-2: Using Offset rule with Lucas numbers

N	U	M	B	E	R	T	H	E	O	R	Y
13	20	12	1	4	17	19	7	4	14	17	24
+	+	+	+	+	+	+	+	+	+	+	+
2	1	3	4	7	11	18	29	47	76	123	199
15	21	15	5	11	28	37	36	51	90	140	223

Step-3: Now applying affine transformation E(x) = (ax+b) mod 26 for a = 5 & b= 20

x	15	21	15	5	11	28	37	36	51	90	140	223
5x+20	95	125	95	45	75	160	205	200	275	470	720	1135
(5x+20) mod 26	17	21	17	19	23	4	23	18	15	2	18	17
Second Encrypted message is	R	V	R	T		E	X	S	P	C	S	R

Step-4: Encrypted message is RVRTXEXSPCSR

Decryption algorithm:

Step-1: First Decrypted Message is RVRTXEXSPCSR

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

Message	R	V	R	T	X	E	X	S	P	C	S	R
y	17	21	17	19	23	4	23	18	15	2	18	17
y-20	-3	1	-3	-1	3	-16	3	-2	-5	-18	-2	-3
21(y-20)	-63	21	-63	-21	63	-336	63	-42	-105	-378	-42	-63
21(y-20)mod26	15	21	15	5	11	2	11	10	25	12	10	15
First Decrypted text	P	V	P	F	L	C	L	K	Z	M	K	P

© 2016, IJMA. All Rights Reserved

Step-3: Reverse Offset rule with the first decrypted message

Message	P	V	P	F	L	C	L	K	Z	M	K	P
	15	21	15	5	11	2	11	10	25	12	10	15
Reverse offset rule with Lucas number	15 - 2	21 - 1	15 - 3	5 - 4	11 - 7	2 - 11	11 - 18	10 - 29	25 - 47	12 - 76	10 - 123	15 - 199
	13	20	12	1	4	-9	-7	-19	-22	-64	-113	-184
Mod 26	13	20	12	1	4	17	19	7	4	14	17	24
Second Decrypted message is	N	U	M	B	E	R	T	H	E	O	R	Y

VIGENERE CIPHER

Encryption algorithm:

Step-1: Let the Plain text be LUCASSERIES

Step-2: Offset rule with Lucas number

L	U	C	A	S	S	E	R	I	E	S
11 + 2	20 + 1	2 + 3	0 + 4	18 + 7	18 + 11	4 + 18	17 + 29	8 + 47	4 + 76	18 + 123
13	21	5	4	25	29	22	46	55	80	141

Using vigenere cipher as second key

C	A	R	D
2	0	17	3

Step-3: Offset rule with the first encrypted message

	13	21	5	4	25	29	22	46	55	80	141
Offset rule with key	13 + 2	21 + 0	5 + 17	4 + 3	25 + 2	29 + 0	22 + 17	46 + 3	55 + 2	80 + 0	141 + 17
	15	21	22	7	27	29	19	49	57	80	158
Mod 26	15	21	22	7	1	3	13	23	5	2	2
Second Encrypted message is	P	V	W	H	B	D	N	X	F	C	C

Step-4: Encrypted message is PVWHBDNXFCC

Decryption algorithm:

Step-1: First Decrypted Message is PVWHBDNXFCC

Step-2: Decrypts with the inverse of vigenere transformation

Message	P	V	W	H	B	D	N	X	F	C	C
	15	21	22	7	1	3	13	23	5	2	2
Reverse Offset rule with key	15 - 2	21 - 0	22 - 17	7 - 3	1 - 2	3 - 0	13 - 17	23 - 3	5 - 2	2 - 0	2 - 17
	13	21	5	4	-1	3	-4	20	3	2	11
Mod 26	13	21	5	4	25	3	22	20	3	2	11
First Decrypted message is	N	V	F	E	Z	D	W	U	D	C	L

© 2016, IJMA. All Rights Reserved

Step-3: Reverse Offset rule with the first decrypted message

Message	N	V	F	E	Z	D	W	U	D	C	L
	13	21	5	4	25	3	22	20	3	2	11
Reverse Offset rule with Lucas number	13 - 2	21 - 1	5 - 3	4 - 4	25 - 7	3 - 11	22 - 18	20 - 14	3 - 47	2 - 76	11 - 123
	11	20	2	0	18	-8	4	-9	-44	-74	-112
Mod 26	11	20	2	0	18	18	4	17	8	4	18
Second Decrypted message is	L	U	C	A	S	S	E	R	I	E	S

PELL NUMBERS

Encryption algorithm:

Step-1: Plain text is SECRETMATHS

Step-2: Offset rule with Pell number

S	E	C	R	E	T	M	A	T	H	S
18 + 0	4 + 1	2 + 2	17 + 5	4 + 12	19 + 29	12 + 70	0 + 169	19 + 408	7 + 985	18 + 2378
18	5	4	22	16	48	82	169	427	992	2396

Step-3: Now applying affine transformation E(x) = (ax+b) mod 26 for a = 5 & b= 12

X	18	5	4	22	16	48	82	169	427	992	2396
5x+12	102	37	32	122	92	252	422	857	2147	4972	11992
(5x+12) mod 26	24	11	6	18	14	18	6	25	15	6	6
Second Encrypted message is	Y	L	G	S	O	S	G	Z	P	G	G

Step-4: Encrypted message is YLGSOSGZPGG

Decryption algorithm:

Step-1: First Decrypted Message is YLGSOSGZPGG

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

Message	Y	L	G	S	O	S	G	Z	P	G	G
y	24	11	6	18	14	18	6	25	15	6	6
y-12	12	-1	-6	6	2	6	-6	13	3	-6	-6
21(y-12)	252	-21	-126	126	42	126	126	273	63	-126	-126
21(y-12)mod26	18	5	4	22	16	22	4	13	11	4	4
First Decrypted text	S	F	E	W	Q	W	E	N	L	E	E

Step-3: Reverse Offset rule with the first decrypted message

Message	S	F	E	W	Q	W	E	N	L	E	E
	18	5	4	22	16	22	4	13	11	4	4
Reverse offset rule with Pell number	18 - 0	5 - 1	4 - 2	22 - 5	16 - 12	22 - 29	4 - 70	13 - 169	11 - 408	4 - 985	4 - 2378
	18	4	2	17	4	-7	-66	-156	-397	-981	-2357
Mod 26	18	4	2	17	4	19	12	0	19	7	18
Second Decrypted message is	S	E	C	R	E	T	M	A	T	H	S

© 2016, IJMA. All Rights Reserved

VIGENERE CIPHERE

Encryption algorithm:

Step-1: Let the Plain text be PELLNUMBERS

Step-2: Offset rule with Pell number

P	E	L	L	N	U	M	B	E	R	S
15	4	11	11	13	20	12	1	4	17	18
+	+	+	+	+	+	+	+	+	+	+
0	1	2	5	12	29	70	169	408	985	2375
15	5	13	16	25	49	82	170	412	1002	2396

Using vigenere cipher as second key

M	A	T	H
12	0	19	7

Step-3: Offset rule with the first decrypted message

	15	5	13	16	25	49	82	170	412	1002	2396
Offset rule with Key	15 + 12	5 + 0	13 + 19	16 + 7	25 + 12	49 + 0	82 + 19	170 + 7	412 + 12	1002 + 0	2396 + 19
	27	5	32	23	37	49	101	177	424	1002	2415
Mod 26	1	5	6	23	11	23	23	21	8	14	23
Second Encrypted message is	B	F	G	X	L	X	X	V	I	O	X

Step-4: Encrypted message is BFGXLXXVIOX

Decryption algorithm:

Step-1: First Decrypted Message is BFGXLXXVIOX

Step-2: Decrypts with the inverse of vigenere transformation

Message	B	F	G	X	L	X	X	V	I	O	X
	1	5	6	23	11	23	23	21	8	14	23
Reverse offset rule with Key	1 - 12	5 - 0	6 - 19	23 - 7	11 - 12	23 - 0	23 - 19	21 - 7	8 - 12	14 - 0	23 - 19
	-11	5	-13	16	-1	23	4	14	-4	14	4
Mod 26	15	5	13	16	25	23	4	14	22	14	4
First Decrypted message is	P	F	N	Q	Z	X	E	O	W	O	E

Step-3: Reverse Offset rule with the first decrypted message

Message	P	F	N	Q	Z	X	E	O	W	O	E
	15	5	13	16	25	23	4	14	22	14	4
Reverse offset rule with Pell number	15 - 0	5 - 1	13 - 2	16 - 5	25 - 12	23 - 29	4 - 70	14 - 169	22 - 408	14 - 985	4 - 2378
	15	4	11	11	13	-6	-66	-155	-386	-971	-2371
Mod 26	15	4	11	11	13	20	12	1	4	17	18
Second Decrypted message is	P	E	L	L	N	U	M	B	E	R	S

© 2016, IJMA. All Rights Reserved

1. Result analysis

S.No	First encryption	Time for first encryption	Super encryption	Time for super encryption
1	PELL NUMBER	1.01 MILLI SEC	Affine or vigenere	3.01 MILLI SEC
2	LUCAS NUMBER	1.3 MILLI SEC	Affine or vigenere	3.35 MILLI SEC

CONCLUSIONS

For multiple encryptions, two different algorithms were performed. Initial encryption is performed with Lucas or Pell numbers using offset rule whereas for super encryption two different ciphers either Affine or Vigenere are performed. In view of the time both are more or less the same.

REFERENCES

1. *"Application of Fibonacci numbers" edited by A.N.Philippou, A.F.Jordan and G.E.Bergun, Springer science media LLC.*
2. *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.*
3. *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 No*
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" IETECH International Journal Of Advanced Computations", Vol: 2 No: 4, PP195-200, 2008.*
6. *"Cryptography: A very short introduction" by Fred Piper and Sean Murthy.*
7. *E.H.Lock Wood, A single-light on pascal's triangle, Math, Gazette 51(1967), PP 243-244.*
8. *Fibonacci, Lucas and Pell numbers andpascal's triangle, Thomas Khoshy, Applied Probability Trust, PP 125-132.*
9. *Fibonacci and Lucas Numbers with applications Thomas Khouhy ISBN: 978-0-471-39969-8.*
10. *J.Buchman"Introduction to cryptography" Springer-Verlag 2001.*
11. *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.*
12. *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.*

Source of support: Nil, Conflict of interest: None Declared

[Copy right © 2016. This is an Open Access article distributed under the terms of the International Journal of Mathematical Archive (IJMA), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.]