Symmetric Key Cryptosystem for Multiple Encryptions

A. ChandraSekhar*,[1], D. Chaya Kumari[2#], S. Ashok Kumar[3*]
[*]*Department of Mathematics GIT, GITAM University, Visakhapatnam, India*
[#]*Department of Mathematics, BVRIT HYDERABAD College of engineering for women, Hyderabad, India*

Abstract
Multiple encryptions is the process of encrypting the plain text more than once. If the plaintext is encrypted twice, then the process of the first encryption is usual encryption and the process of second-time encryption is referred as the super-encryption. For multiple encryptions, same or different algorithms can be used. If the same key is used for multiple encryptions, for an attacker it is not that hard to recover the plain text. In this paper, a symmetric cryptosystem is proposed using Fibonacci numbers for the first level of encryption and Affine or Vigenere *transformation is employed for super encryption.*

Keywords
Fibonacci numbers, Affine, Vigenere *transformations.*

I. INTRODUCTION

Super-encryption is a process of encrypting the information that is already encrypted [5][13]. 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 a comparatively weak algorithm.

In view of enhancing the security levels multiple encryptions were introduced. By using same algorithms for the generation of the single for both the encryptions is vulnerable. In order to overcome this problem, the recent researchers suggest using keys which are stochastically independent. It is evident from the history that any cipher can be breakable except the one time pad.

II. FIBONACCI NUMBERS

The Fibonacci sequence is 1, 1, 2, 3, 5, 8. . . [1][7][8] where each entry is formed by adding the two previous ones, starting with 1 and 1 as the first two terms. Fibonacci numbers can be generated from following recurrence relation $F_{n+1} = F_n + F_{n-1}$ with $F_1 = F_2 = 1$.

I.1 Affine Cipher

An affine enciphering transformation is $C \equiv aP + b \mod N$ 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 $y - b \equiv ax \mod 26$ or equivalently $ax \equiv y - b \mod 26$.

I.2 *Vigenere* cipher

The Vigenere cipher was generated by Giovan Batista Belaso in 1553[9]. Thiscipher 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 Vigenereciphers are more powerful than substitution ciphers.

III.PRESENT WORK

Multiple Encryptions
Encryption algorithm:
Step-1: Alice creates plain text is P = $p_1p_2, p_3 \ldots p_m$
Step-2: Alice uses the offset rule with Fibonacci numbers F=$f_1,f_2,f_3 \ldots f_n$ to each value in sequential order to get the1^{sr}ciphertext.

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

Step-4: Now Alice perform super encryption with the Affine transformation(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 the 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: Bob reverses the offset rule with Fibonacci number from the first decrypted message to get the original plaintext.

SUPER ENCRYPTION OF* VIGENERE *CIPHER
Encryption algorithm:

Step-1: Alice creates plaintexts P = $p_1p_2,p_3 \ldots\ldots p_m$

Step-2: Alice uses offset rule with Fibonacci numbers $F=f_1f_2f_3\ldots f_n$ to each value in sequential order and get 1[sr]ciphertext

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

Step-4: Now Alice performs Vigenere transformation use offset rule with
to the numerical value of each letter of a secret keyword to first level encryption message.

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

Decryption algorithm:

Step-1: Bob receives the super-encrypted message.

Step-2: Bob decrypts with the inverse Vigenere transformation to super encryption message. It is the first decryption message

Step-3:Bob uses reverse offset rule with Fibonacci number from the first decrypted message to get original plaintext.

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 CRYPTOGRAPHY

Step-2: Offset rule with Fibonacci numbers

C	R	Y	P	T	O	G	R	A	P	H	Y
2 + 1	17 + 1	24 + 2	15 + 3	19 + 5	14 + 8	3 + 13	17 + 21	0 + 34	15 + 55	7 + 89	24 + 144
3	18	26	18	24	22	19	38	34	70	96	168

Step-3: Now applying affine transformation E(x)=(ax+b) mod 26 for a = 5 & b= 8

x	3	18	26	18	24	22	19	38	34	70	96	168
5x+8	23	98	138	98	128	118	103	198	178	358	488	848
(5x+8) mod 26	23	20	8	20	24	14	25	16	22	20	20	16
Second Encrypted message is	X	U	I	U	Y	O	Z	Q	W	U	U	Q

Step-4:Encrypted message is XUIUYOZQWUUQ

Decryption algorithm:

Step-1:First decrypted Message **is** XUIUYOZQWUUQ

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

Message	X	U	I	U	Y	O	Z	Q	W	U	U	Q
y	23	20	8	20	24	14	25	16	22	20	20	16

y-8	15	12	0	12	16	6	17	8	14	12	12	8
21(y-8)	315	252	0	252	336	126	357	168	394	252	252	168
21(y-8)mod26	3	18	0	18	24	22	19	12	8	18	18	12
First decrypted message	D	S	A	S	Y	W	T	M	I	S	S	M

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

Message	D	S	A	S	Y	W	T	M	I	S	S	M
	3	18	0	18	24	22	19	12	8	18	18	12
Reverse Offset rule with Fibonacci number	3 - 1	18 - 1	0 - 2	18 - 3	24 - 5	22 - 8	19 - 13	12 - 21	8 - 34	18 - 55	18 - 89	12 - 144
	2	17	-2	15	19	14	3	-9	-26	-37	-71	-132
Mod 26	2	17	24	15	19	14	3	17	0	15	7	24
Second decrypted message is	C	R	Y	P	T	O	G	R	A	P	H	Y

VIGENERE CIPHER

Encryption algorithm:

Step-1: Let the Plain text be MATHEMATICS

Step-2: Offset rule with Fibonacci number

M	A	T	H	E	M	A	T	I	C	S
12 + 1	0 + 1	19 + 2	7 + 3	4 + 5	12 + 8	0 + 13	19 + 21	8 + 34	2 + 55	18 + 89
13	1	21	10	9	20	13	40	42	57	107

Using* Vigenere *ciphers for key

G	I	T	A	M
6	8	19	0	12

Step-3:Offset rule with the first decrypted message

	13	1	21	10	9	20	13	40	42	57	107
	13	1	21	10	9	20	13	40	42	57	107

Offset rule with Key	+ 6	+ 8	+ 19	+ 0	+ 12	+ 6	+ 8	+ 19	+ 0	+ 12	+ 6
	19	9	40	10	21	26	21	59	42	69	113
Mod 26	19	9	14	10	21	0	21	7	16	17	9
Second Encrypted message is	T	J	O	K	V	A	V	H	Q	R	J

Step-4: Encrypted message is TJOKVAVHQRJ

Decryption algorithm:

Step-1: First Decrypted Message **is** TJOKVAVHQRJ

Step-2: Decrypts with the inverse of Vigenere transformation

Message	T	J	O	K	V	A	V	H	Q	R	J
	19	9	14	10	21	0	21	7	16	17	9
Reverse Offset rule with Key	19 - 6	9 - 8	14 - 19	10 - 0	21 - 12	0 - 6	21 - 8	7 - 19	16 - 0	17 - 12	9 - 6
	13	1	-5	10	9	-6	13	-12	16	5	3
Mod 26	13	1	21	10	9	20	13	14	16	5	3
First Decrypted message	N	B	V	K	J	U	N	O	Q	F	D

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

Message	N	B	V	K	J	U	N	O	Q	F	D
	13	1	21	10	9	20	13	14	16	5	3
Reverse Offset rule with Fibonacci number	13 - 1	1 - 1	21 - 2	10 - 3	9 - 5	20 - 8	13 - 13	14 - 21	16 - 34	5 - 55	3 - 89
	12	0	19	7	4	12	0	-7	-18	-50	-86
Mod 26	12	0	19	7	4	12	0	19	8	2	18
First Decrypted message	M	A	T	H	E	M	A	T	I	C	S

IV. CONCLUSIONS

For multiple encryptions, two different algorithms were performed. Initial encryption is performed with Fibonacci numbers using offset rule whereas for super encryption two different ciphers either Affine or Vigenere are performed. In view of the known attack both are more or less the same.Further the keys generated at two levels are stochastically independent. To enhance the security levels, two different keys are applied.

REFERENCES

[1] *"Application of Fibonacci numbers" edited by A.N.Philippou, A.F.Jordan and G.E.Bergun, Springer science media LLC.*

[2] *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*

[3] *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.*

[4] *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.*

[5] *"Cryptography: A very short introduction" by Fred Piper and Sean Murthy.*

[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 Khouhy ISBN: 978-0-471-39969-8.*

[9] *J.Buchman"Introduction to cryptography" Springer-Verlag 2001.*

[10] *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.*

[11] *K.H.Rosen "Elementary number theory and its applications" Third edition, Addison Wesly.*

[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.*

[13] *Neal Koblitz" A course in number theory and cryptography"IBSN 3-578071-8 SPIN 10893308.*

[14] *B. Ravi Kumar , A. Chandra Sekhar , G.Appala Naidu "A Novel ElGamal Encryption Scheme of Elliptic Curve Cryptography". International Journal of Computer Trends and Technology (IJCTT) V20(2):70-73, Feb 2015. ISSN:2231-2803.*