RESEARCH ARTICLE OPEN ACCESS

Exchange of Message using Fourier Sine Transforms via Affine Transformation

Archana K N[1], Suman K R[2]
1(Department of Mathematics, AMC Engineering College,Banglore
Email: archanabaangre68@gmail.com)
2 (Department of Mathematics, AMC Engineering College,Banglore
Email : sumankangokar123@gmail.com)

Abstract:

In this paper, we established an application of Fourier sine transformation in exchanging the message in a secured channel via affine cryptosystem which is helpful in digital electronics and signal processing.

***Keywords* - Decryption, Encryption, Fourier sine transform, Modulo function.**

I. INTRODUCTION

Definition: Fourier sine transform [7] is an integral transform that are mainly applicable for signal processing or statistics. If f(x) is defined for all positive values of x.
If f(x) is defined for all positive values of x.

$$F_s[f(x)] = \int_0^\infty f(x)\sin(ux)\,dx = F_s[u]$$

Inverse Fourier sine transform is given by.

$$f(x) = \frac{2}{\pi}\int_0^\infty F_s(u)\sin(ux)du$$

Properties of Fourier Sine Transforms:

1. Linearity Property:
   $F_s[a\ f(x) \pm b\ g(x)] = a\,F_s\,[f(x)] \pm b\,F_s$

2. Change of Scale Property:
   [illegible]

3. Modularity Property of Fourier Sine Transforms:

$$[\ (\ )\qquad] = \frac{1}{2}[F\ (u-a) - F_c(u+a)]$$

$$F_s[f(x)cosax] = \frac{1}{2}[F_s(u+a) + F_s(u-a)]$$

Cryptography: Cryptography is the science of using mathematics to hide the information. It allows us to store sensitive information or to transmit it over insecure network, so that it can only be read by the intended reciptant.
Plaintext: Information that can be directly read.
Ciphertext: Encrypted data of plaintext is ciphertext.
Encryption: Process of converting plaintext to ciphertext.
Decryption: Process of reverting ciphertext to plain text.

Cryptography mainly classified in to 3 types:

1. Symmetric / private key cryptography uses single key for both encryption and decryption.
2. Hash functions: it is one way function which is infeasible practically to reverse the computation. These are the basic tools of modern cryptography [5].
3. Asymmetric / public key cryptography uses different keys for encryption and decryption.

In this paper, we propose a method of exchanging the message using Fourier sine transform via affine cryptosystem.
The plain text and ciphertext are broken up into message units. A message unit can be a single letter, also called monograph, a pair of letters called digraph, a triple of letters called trigraph or a block of more than 3 letters called multigraph [3].
Affine transformation is one of the types of symmetric key cryptosystems.

Affine transformation is defined as follows:
$C = f(p) = ap + b\ (mod\ N)$ where 'P' is the plaintext and 'C' is the cipher text respectively. a, b and N are positive integers and 'f' is a mapping from P to C.

The plaintext 'P' can be recovered from the given cipher text 'C' i.e.,
$P = a^{-1}(C - b)(mod\ N)$
$P = a^{-1}C - a^{-1}b(mod\ N)$
$= {}_1 + {}_2(\qquad)$
where $k_1 = a^{-1}$ and $k_2 = -a^{-1}b$ and a^{-1} is the inverse of 'a'.

Theorem: Given the affine map $C \equiv ap + b \ (mod\ N)$ where $a\ \epsilon (^{Z}/\quad)^{*}$, $b\ \epsilon (^{Z}/\quad)$. The transformation gives a unique value of 'p' for a given C iff gcd (a, N) = 1 and that the total number of affine transformations is given by $N.\emptyset(N)$, where $\emptyset$ is Euler-phi function [2].

Encryption Algorithm:
Step 1: Consider the plain text MATHEMATICS and write the numerical equivalents.
Step 2: Choose 'a' and 'b' in affine transformation $ax +$ ( ) such that (,) = 1 (,) = 1
Step 3: Now consider Fourier sine transformation and substitute the obtained numerical value of cipher text for "*a*" in the Fourier sine transform $\int_0^\infty e^{-ax} \sin(ux)\, dx$ and sender sends this ciphered message to receiver.

Decryption Algorithm:
Step 1: Receiver receives the cipher text and first decrypt by using inverse Fourier sine transformation.

Step 2: By the obtained text from step 1 receiver again decrypts the cipher text using inverse affine transformation and with suitable decryption key.
Step 3: Receiver can retrieve the plain text.

EXAMPLE:
Consider the plain text "MATHEMATICS" write the numerical equivalent of each alphabet by taking *a* = 7, *b* = 6 in affine transformation ("ax + b"), we get

M	A	T	H	E	M	A	T	I	C	S
12	0	19	7	4	12	0	19	8	2	18
(7x+6) mod26										
12	6	9	3	8	12	6	9	10	20	2

Calculations of (7x+6) mod 26:

Alphabet	Numerical equivalent	(7x + 6) mod 26	Value
M	12	(7(12) + 6) mod 26	12
A	0	(7(0) + 6) mod 26	6
T	19	(7(19) + 6) mod 26	9
H	7	(7(7) + 6) mod 26	3
E	4	(7(4) + 6) mod 26	8
M	12	(7(12) + 6) mod 26	12
A	0	(7(0) + 6) mod 26	6
T	19	(7(19) + 6) mod 26	9
I	8	(7(8) + 6) mod 26	10
C	2	(7(2) + 6) mod 26	20
S	18	(7(18) + 6) mod 26	2

Again, by using Fourier sine transform encrypt the obtained numerical values as 'a' in the Fourier sine transform $\int_0^\infty e^{-ax} \sin(\ )$

i.e., $\frac{\pi}{2}\int_0^\infty e^{-12x} \sin(ux)\, dx$, $\frac{\pi}{2}\int_0^\infty e^{-6x} \sin(ux)\, dx$,
$\frac{\pi}{2}\int_0^\infty e^{-9x} \sin(ux)\, dx$, $\frac{\pi}{2}\int_0^\infty e^{-3x} \sin(ux)\, dx$,
$\frac{\pi}{2}\int_0^\infty e^{-8x} \sin(ux)\, dx$, $\frac{\pi}{2}\int_0^\infty e^{-12x} \sin(ux)\, dx$,
$\frac{\pi}{2}\int_0^\infty e^{-6x} \sin(ux)\, dx$, $\frac{\pi}{2}\int_0^\infty e^{-9x} \sin(ux)\, dx$
$\frac{\pi}{2}\int_0^\infty e^{-10x} \sin(ux)\, dx$, $\frac{\pi}{2}\int_0^\infty e^{-20x} \sin(ux)\, dx$,
$\frac{\pi}{2}\int_0^\infty e^{-2x} \sin(ux)\, dx$

and sender sends cipher text as

$$[\frac{12}{2(\ ^2 + 144)}, \frac{6}{2(\ ^2 + 36)}, \frac{9}{2(\ ^2 + 81)}, \frac{3}{2(\ ^2 + 9)}, \frac{8}{2(\ ^2 + 64)}, \frac{12}{2(\ ^2 + 144)}, \frac{6}{2(\ ^2 + 36)}, \frac{9}{2(\ ^2 + 81)}, \frac{10}{2(\ ^2 + 100)}, \frac{20}{2(\ ^2 + 400)}, \frac{2}{2(\ ^2 + 4)}]$$

We made Fourier sine transformation as public key and affine transformation as private key to decrypt the message.

Decryption:
Recipient receives the message from the sender and first decrypt by using inverse Fourier sine transformation and get decrypts as

$[e^{-12x}, e^{-6x}, e^{-9x}, e^{-3x}, e^{-8x}, e^{-12x}, e^{-6x}, e^{-9x}, e^{-10x}, e^{-20x}, e^{-2x}]$

Again, by using private key as affine transformation with $E^{-1}(y) = 15(y-6) mod\ 26$

y	12	6	9	3	8	12	6	9	10	20	2
y-6	6	0	3	-3	2	6	0	3	4	14	-4
15(y-6)	90	0	45	-45	30	90	0	45	60	210	-60
Mod26	12	0	19	7	4	12	0	19	8	2	18

In this manner, we can exchange the message in a secured channel, which is more secure than the symmetric key cryptosystem.

II. CONCLUSION

We can extend this encryption scheme by using Z-transformation and by using any symmetric key cryptosystem like vignere cipher etc, as private key.

III. REFERENCES

[1] C. Manjula, Chaya Kumari, Kavya B S," Exchange of message using, Fourier sine transforms Via Affine transformation.

[2] A.K. Bhandari, The public key cryptography. Proceedings of the advanced instructional workshop on algebraic number theory HBA (2003) 287-301.

[3] Neil Koblitz, A course in number theory and cryptography ISBN 578071-8 SPIN 10893308

[4] G.P. Tolstoy, Fourier Series, Dover, 1972.

[5] T.W. Korner, Fourier Analysis, Cambridge University Press, 1988.

[6] Buchmann, Introduction to cryptography, Springer Verlag 2001.

[7] Alfred J. Menezes, Paul C. Van Oorschot and Scott A.Vanstone,Handbook of Applied Cryptography 1st edition. CRC Press.

[8] Ronald Newbold Bracewell, Fourier transform and its applications, 3rd edition, McGraw Hill 2000.

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

[10] Tom M .Apostol, Introduction to analytic number theory, springer Verlag, Newyork.

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

[12] Thomas Khoshy, Fibonacci and Lucas numbers with applications, John Wiley and Sons,NY,2001,ISBN: 978-0-471-39939-8.

[13] A. Terras, Fourier Analysis on Finite Groups and Applications, Cambridge University Press, 1999

[14] Chaya Kumari. D and S. Ashok Kumar, Redei rational functions as Permutation functions and an algorithm to compute Redei rational, functions IJESM vol:8, issue 2 Feb 2019.

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

[16] A. Chandra Sekhar, 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.

[17] A. Chandra Sekhar, D. Chaya Kumari, Ch. Pragathi, S. Ashok Kumar, Multiple Encryptions of Fibonacci Lucas Transformations, International Organization of Scientific Research (IOST)e-ISSN: 2278-5728. Volume 12, Issue 2 Ver. II (Mar. - Apr. 2016), PP 66-72.

[18] 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.

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

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

[21] A. Chandra Sekhar, D. Chaya Kumari, Ch. Pragathi, S. Ashok Kumar, Multiple Encryption of Independent Ciphers, International Journal of Mathematical Archive (IJMA) –V 7(2), 2016, 103-110.

[22] P.A. Kameswari, R.C. Kumari, Cryptosystem with Redei rational functions via pellconics IJCA (0975-8887) VOL 54, NO:15.

[23] Chaya Kumari. D, Triveni. D and S. Ashok Kumar, Super encryption method of Laplace transformations using Fibonacci numbers. Journal of Hauzhong University of Science and Technology 50(7).

[24] James L. Massey, The Discrete Fourier Transform in Coding and Cryptography, ITW 1998, San Diego, CA. 2011.