International Journal of Mathematics Trends and Technology
ISSN: 2231 – 5373 / https://doi.org/10.14445/22315373/IJMTT-V68I3P503
Volume 68 Issue 3, 11-14, March 2022

Original Article

Exchange of Message using Fourier Transforms Via Affine Transformation

C. Manjula[1], Chaya Kumari Divakarla[2], Kavya B S[3]

[1,2]*Associate professor in Mathematics, AMC Engineering college, Bangalore.*
[3]*Assistant professor in Mathematics, AMC Engineering college, Bangalore.*

Received Date: 17 February 2022
Revised Date: 25 March 2022
Accepted Date: 27 March 2022

Abstract - *In this paper, we established an application of Fourier cosine 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 cosine transform, Modulo function.*

I. INTRODUCTION

Definition: Fourier cosine 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;

$$F_C[f(x)] = \int_0^\infty f(x)\cos(ux)\,dx = F_c[u]$$

Inverse Fourier cosine transform is given by

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

Properties of Fourier Cosine Transforms:

[1] Linearity Property :

$$F_c[C_1 f_1(x) + C_2 f_2(x) + \dots\dots\dots.. + C_n f_n(x)] = C_1 F_c[f_1(x)] + C_2 F_c[f_2(x)] + \cdots + C_n F_c[f_1(x)]$$

[2] Change of Scale Property :

If $F_c[(x)] = C_1 F_c(u)$ then $F_c[f(ax)] = \frac{1}{a} F_c\left(\frac{u}{a}\right)$

[3] Modularity Property Of Fourier Cosine Transforms :

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

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

Cryptography: Cryptography is a technique of sending information and communications through use of codes [2]. It is the science used to try to keep information secret and safe. Modern cryptography is a mix of mathematics, computer science and electrical engineering.

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 with Fourier cosine 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.,

$P = a^{-1}(C - b)(mod\ N)$

$P = a^{-1}C - a^{-1}b(mod\ N)$

$P = k_1C + k_2(mod\ N)$ 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 $a\ \epsilon \left({}^{Z}/_{NZ}\right)^{*}$, $b\ \epsilon \left({}^{Z}/_{NZ}\right)$. 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 KNOWLEDGE and write the numerical equivalents

Step 2: Choose ‘a’ and ‘b’ in affine transformation $ax + b(mod\ N)$ such that $(a, N) = 1\ and\ (b, N) = 1$

Step 3: Now consider Fourier cosine transformation and substitute the obtained numerical value of cipher text for “a” in the Fourier cosine transform $\int_0^\infty e^{-ax} \cos(sx)\, dx$ and sender sends this ciphered message to receiver.

Decryption Algorithm:

Step 1: Reciever receives the cipher text and first decrypt by using inverse Fourier cosine 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 "KNOWLEDGE" write the numerical equivalent of each alphabet by taking a = 5, b = 8 in affine transformation ("ax+b"), we get

K	N	O	W	L	E	D	G	E
10	13	14	22	11	4	3	6	4
(5x+8)mod26								
6	21	0	14	11	2	23	12	2

Calculations of (5x+8) mod 26 :

Alphabet	Numerical equivalent	(5x+8)mod26	Value
K	10	5(10) + 8 mod 26	6
N	13	5(13) + 8 mod 26	21
O	14	5(14) + 8 mod 26	0
W	22	5(22) + 8 mod 26	14
L	11	5(11) + 8 mod 26	11
E	4	5(4) + 8 mod 26	2
D	3	5(3) + 8 mod 26	23
G	6	5(6) + 8 mod 26	12
E	4	5(4) + 8 mod 26	2

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

i.e., $\frac{\pi}{2}\int_0^\infty e^{-6x}\cos(sx)\,dx$, $\frac{\pi}{2}\int_0^\infty e^{-21x}\cos(sx)\,dx$, $\frac{\pi}{2}\int_0^\infty e^{-0x}\cos(sx)\,dx$, $\frac{\pi}{2}\int_0^\infty e^{-14x}\cos(sx)\,dx$, $\frac{\pi}{2}\int_0^\infty e^{-11x}\cos(sx)\,dx$, $\frac{\pi}{2}\int_0^\infty e^{-2x}\cos(sx)\,dx$, $\frac{\pi}{2}\int_0^\infty e^{-23x}\cos(sx)\,dx$, $\frac{\pi}{2}\int_0^\infty e^{-12x}\cos(sx)\,dx$, $\frac{\pi}{2}\int_0^\infty e^{-2x}\cos(sx)\,dx$ and sender sends cipher text as

$$\left[\frac{6\pi}{2(s^2+36)},\frac{21\pi}{2(s^2+36)},\frac{0.\pi}{2(s^2+36)},\frac{14\pi}{2(s^2+36)},\frac{11\pi}{2(s^2+36)},\frac{2\pi}{2(s^2+36)},\frac{23\pi}{2(s^2+36)},\frac{12\pi}{2(s^2+36)},\frac{2\pi}{2(s^2+36)}\right]$$

We made Fourier cosine 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 cosine transformation and get decrypts as
$[e^{-6x}, e^{-21x}, e^{-0x}, e^{-11x}, e^{-2x}, e^{-23x}, e^{-12x}, e^{-2x}]$

Again by using private key as affine transformation with $E^{-1}(y) = 21(y-8) mod\ 26$

y	6	21	0	14	11	2	23	12	2
y-8	-2	13	-8	6	3	-6	15	4	-6
21(y-8)	-42	273	168	126	63	-126	315	84	-126
Mod26	10	13	14	22	11	4	3	6	4

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

CONCLUSION

We can extend this encryption scheme by using Fourier sine transformation also and by using any symmetric key cryptosystem like vignere cipher etc; as private key.

REFERENCES

[1] A.K. Bhandari, The public key cryptography. Proceedings of the Advanced Instructional Workshop on Algebraic Number Theory HBA (2003) 287-301.
[2] Neil Koblitz, A Course in Number Theory and Cryptography ISBN 3-578071-8 SPIN 10893308.
[3] G.P. Tolstov, Fourier Series, Dover, (1972).
[4] T.W. Korner, Fourier Analysis, Cambridge University Press, (1988).
[5] J.Buchmann, Introduction to Cryptography, Springer verlag (2001).
[6] Alfred J. Menezes, Paul C.Van Oorschot and Scott A.Vanstone,Handbook of Applied Cryptography 1st edition. CRC Press
[7] Ronald newbold bracewell, Fourier transform and its applications, 3rd edition, Mcgraw Hill, (2000).
[8] A.P.Stakhov, The Golden section and Modern Harmony Mathematics, Applications of Fibonacci numbers, kluwer Academic publishers (1998) 393-399
[9] Tom M .Apostol, Introduction to Analytic Number Theory, Spriger-Verlag, Newyork.
[10] Thomas Khoshy, Fibonacci, Lucas and Pell Numbers and Pascal's triangle, Applied Probability Trust, 125-132.
[11] Thomas Khoshy, Fibonacci and Lucas numbers with Applications, John Wiley and Sons,NY,(2001).ISBN: 978-0-471-39939-8.
[12] A. Terras, Fourier Analysis on Finite Groups and Applications, Cambridge University Press, (1999).
[13] Chaya Kumari. D and S. Ashok Kumar, Redei Rational Functions as Permutation Functions and an Algorithm to Compute Redei Rational Functions IJESM , 8(2) (2019).
[14] E.H.Lock Wood, A single-light on pascal's triangle, Math, Gazette, 51(1967) 243-244.
[15] A.Chandra Sekhar, D. Chaya Kumari, S.Ashok Kumar, Symmetric Key Cryptosystem for Multiple Encryptions, International Journal of Mathematics Trends and Technology (IJMTT)., 29(2) (2016) 140-144 . ISSN:2231-5373.
[16] 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,. 12(2) (2016) 66-72.
[17] K.R.Sudha, A. Chandra Sekhar, P.V.G.D, Prasad Reddy, Cryptographic Protection Of Digital Signal Using some Recurrence Relations, IJCNS, (2007) 203-207.
[18] A. Chandra Sekhar, V. Anusha, B. Ravi Kumar and S. Ashok Kumar, Linear independent spanning sets and Linear Transformations for multi-level encryption, 36(4) (2015) 385.
[19] Tianping Zhang and Yuankui Ma, On Generalized Fibonacci Polynomials and Bernouli Numbers Journal of Integer sequence, 8 (2015) 1-6.
[20] A.Chandra Sekhar, D. Chaya Kumari, Ch.Pragathi, S. Ashok Kumar, Multiple Encryption of Independent Ciphers, International Journal of Mathematical Archive (IJMA) , 7(2) (2016) 103-110.
[21] P.A. Kameswari, R.C. Kumari, Cryptosystem with Redei rational functions via pellconics IJCA(0975-8887) , 54(15).
[22] 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).
[23] James L. Massey, The Discrete Fourier Transform in Coding and Cryptography, ITW 1998, San Diego, CA. (2011).
[24] J.M. Ash(ed.), Studies in Mathematical Association of America, (1976).
[25] D Boneh, X Boyen,and H Shacham, Short group Signatures, Annual International Cryptology Conference , (2004).