International Journal of Mathematical Archive-10(7), 2019, 32-36
Available online through www.ijma.info ISSN 2229 – 5046

CONTRIBUTION OF LAPLACE TRANSFORM IN CRYPTOGRAPHY

DR. H. K. UNDEGAONKAR*
Assistant Professor, Department of Mathematics,
Bahirji Smarak Mahavidyalaya, Basmathnagar, India.

DR. R. N. INGLE
Principal & Associate Professor, Department of Mathematics,
Bahirji Smarak Mahavidyalaya, Basmathnagar, India.

(Received On: 12-06-19; Revised & Accepted On: 03-07-19)

ABSTRACT

In this paper we introduce the application of Laplace transform &Inverse Laplace transform in the process of encryption and decryption respectively. In the first part of the paper we consider the plain text and converts it to cipher text by applying Laplace transform to trigonometric cosine function and in the second part we converts cipher text to plain text by applying inverse Laplace transform .Finally we generalize some results regarding encryption and decryption.

Keywords: *Laplace Transform, Encryption, Decryption, Cryptography.*

1.1 INTRODUCTION

There are various applications of integral transforms in applied Mathematics & in engineering field [1, 2]. We know that Laplace transform is an integral transform which is widely used in solving linear ordinary and partial differential equations. [3]. There is a contribution of Laplace transform in evaluating some complicated definite integrals. [10]. Laplace transform is one of the oldest and commonly used integral transform available in literature. Laplace transform technique was developed by the French Mathematician Pierre Simon de Laplace in 1779 [1]. It is a very powerful tool applied in various areas like Engineering and other Sciences.

1.2 SOME USEFUL DEFINITIONS AND THEOREMS

Def.1.2.1 Laplace transforms: we define Laplace transform of $g(y)$ by

$$L[g(y)] = F(p) = \int_0^\infty e^{-py}\, g(y)dy. \text{ , Re (p)} > 0$$

Where $e^{-py}$the kernel of this transform and p is is the transform variable which is a complex number.

Def.1.2.2 Inverse Laplace transform: If F(p)is the Laplace transform of f(x) then the inverse Laplace transform of F(p) is f (x) and we write $L^{-1}\{F(p)\} = f\,(x)$.

Definition 1.2.3: Cryptology: It is the study of secrecy systems which can be traced back to the early Egyptians.

Definition 1.2.4: Plain text: The original message which is to be transmitted in such a form having secrecy.

Definition 1.2.5: Cipher text: when we convert the original message in the form having secrecy then this new form is said to be cipher text.

Definition 1.2.6: cipher: The method of converting plain text to cipher text is called cipher.

Definition 1.2.7: Encrypting: The process of converting plain text to cipher text is known as encrypting.

Definition 1.2.8: Decrypting: The reverse process by the beneficiary who knows key is known as decrypting and is accomplished by a decrypt.

Corresponding Author: Dr. H. K. Undegaonkar*
Assistant Professor, Department of Mathematics,
Bahirji Smarak Mahavidyalaya, Basmathnagar, India.

There are various methods for creation of cipher text in the literature.

Theorem 1.1.1: [6] Let $H_0, H_1\ H_2 H_3, H_4, \ldots\ldots$ be coefficients of $t^2 \sinh 2t$ then given plaintext in terms of H_i i=0, 1, 2, 3, 4,…… under Laplace transform of $Ht^2 \sinh 2t$ can be converted to cipher text $H_i{}' = r_i - 26k_i$ for i =0, 1, 2, 3,……. where $r_i = 2^{2i+1}(2i+2)(2i+3)H_i$ for i=0, 1, 2, 3, 4… and a key is given by

$$k_i = \frac{r_i - H_i{}'}{26} \text{ for } i = 0, 1, 2, 3, 4\ldots$$

Theorem 1.1.2: [6] The given cipher text in terms of $H_i{}'$ With a given key k_i for $i = 0,1,2,3,4, \ldots\ldots$ can be converted to plain text H_i under the inverse Laplace transform of

$$H\frac{d2}{dp2}\frac{2}{p^2-2^2} = \sum_{i=0}^{\infty}\frac{r_i}{p^{2i+4}} \quad \text{where} \quad H_i = \frac{26k_i + H_i{}'}{2^{2i+1}(2i+2)(2i+3)} \text{ for i=0, 1, 2, 3, 4…... and } r_i = 26k_i + H_i{}'$$

2 CONVERSION OF PLAINTEXT TO CIPHER TEXT BY APPLYING LAPLACE TRANSFORM TO TRIGONOMETRIC COSINE FUNCTIONS

(2.1) Suppose that we are given A.B.C.D, …………,Z as a plaintext and to convert it to cipher text in this method we have to give the following allotment to letters in the given plaintext.
A→0,B→1,C→2,D→3,E→4,F→5,G→6,H→7,I→8,J→9,K→10,L→11,M→12,N→13,O→14,P→15,Q→16 ,R→17,S→18,T→19,U→20,V→21,W→22,X→23,Y→24,Z→2

In this section we will apply Laplace transform to trigonometric cosine function for the process of encryption

Also we will convert cipher text to plaintext by applying inverse Laplace transform
Consider the cosine series given by

$$\cos nx = 1 - \frac{n^2x^2}{2!} + \frac{n^4x^4}{4!} - \frac{n^6x^6}{6!} + \frac{n^8x^8}{8!} - \frac{n^{10}}{10!}.x^8 \text{................then we have}$$

$$x^m \cos nx = x^m - \frac{n^2x^{m+2}}{2!} + \frac{n^4x^{n+4}}{4!} - \frac{n^6x^{m+6}}{6!} + \ldots \tag{2.1}$$

Suppose that $C_0, C_{1,}, C_2, C_3, C, C_5, I_6, C_7, \ldots\ldots C_j$ be coefficients of theeq$^{\mathbf{n}}$ (2.1) then we write this new equation as

$$Cx^m \cos nx = c_0x^m - c_1\frac{n^2x^{m+2}}{2!} + c_2\frac{n^4x^{m+4}}{4!} - c_3\frac{n^6x^{m+6}}{6!} + \ldots \tag{2.2}$$

Ex. 2.1.1: Let us consider the plaintext given by

G O O G L E and by our allotment be equivalent to
6 14 14 6 11 4

Case-(i): when m=1& n=1eq$^{\mathbf{n}}$ (2.2) becomes

$$Cx \cos x = c_0\, x - c_1\frac{x^3}{2!} + c_2\frac{x^5}{4!} - c_3\frac{x^7}{6!} + \ldots\ldots\ldots\ldots\ldots\ldots \tag{2.3}$$

Let us assume that $c_0 = 6, c_1 = 14, c_2 = 14, c_3 = 6, c_4 = 11, c_5 = 0, c_6 = 11$, be coefficients of the above eq$^{\mathbf{n}}$ (2.3)

$$\therefore Cx \cos x = 6\,x - 14\frac{x^3}{2!} + 14\frac{x^5}{4!} - 6\frac{x^7}{6!} + 11\frac{x^9}{8!} - 4\frac{x^{11}}{10!} \tag{2.4}$$

Applying Laplace transform to the above eq$^{\mathbf{n}}$ it changes to

$$L\{Cx\cos x\} = 6L(x) - 14L\left(\frac{x^3}{2!}\right) + 14L\left(\frac{x^5}{4!}\right) - 6L\left(\frac{x^7}{6!}\right) + 11L\left(\frac{x^9}{8!}\right) - 4L\left(\frac{x^{11}}{10!}\right)$$

$$L\{Cx\cos x\} = \frac{6}{p^2} - \frac{42}{p^4} + \frac{70}{p^6} - \frac{42}{p^8} + \frac{99}{p^{10}} - \frac{44}{p^{12}} \tag{2.5}$$

Suppose that $r_0 = 6,\ r_1 = 42,\ r_2 = 70, r_3 = -42,\ r_4 = 99,\ r_5 = -44$

Let us determine $C_i{}'$ such that $r_i \equiv C_i{}' \bmod 26$
$6 \equiv -20 \bmod 26$, $-42 \equiv 10 \bmod 26$, $70 \equiv -8 \bmod 26$, $-42 \equiv 10 \bmod 26$
$99 \equiv -5 \bmod 26$, $-44 \equiv 8 \bmod 26$

Let $c_0{}' = -20,\ c_1{}' = 10,\ c_2{}' = -8,\ c_3{}' = 10,\ c_4{}' = -5,\ c_5{}' = 8$

Assuming the values of $c_0{}', c_1{}', c_2{}', \ldots\ldots\ldots, I_5{}'$ to be non-negative the given plaintext G O O G L E is converted to the cipher text
-20 10 -8 10 -5 8

The following table gives key for beneficiary to crack the cipher text.

Table − 2.1

i	C_i	$r_i = (-1)^i(2i+1)C_i$	$k_i = \frac{r_i - C_i{}'}{26}$	$C_i{}' = r_i - 26k_i$
0	6	6	1	−20
1	14	−42	−2	10
2	14	70	3	−8
3	6	−42	-2	10
4	11	99	4	−5
5	4	−44	-2	8

From the above table we have the generalization given below.

Theorem 2.1.1: Suppose that $C_0, C_1, C_2, \cdots\cdots, C_J$ are coefficients of $x\cos x$ .Then under the Laplace transform of $Cx\cos x$ the given plaintext C_i Can be converted to cipher text $C_i{}' = r_i - 26k_i$
where $r_i = (-1)^i(2i+1)C_i$ and key is given by $k_i = \frac{r_i - C_i{}'}{26}$ for $i = 0, 1, 2, 3 \ldots\ldots..$

By operating inverse Laplace transform. to (2.5) we have

$$L^{-1}\{L\{Cx\cos x\}\} = 6L^{-1}\left[\frac{1}{p^2}\right] - 42L^{-1}\left[\frac{1}{p^4}\right] + 70\left[\frac{1}{p^6}\right] - 42L^{-1}\left[\frac{1}{p^8}\right] + 99\,L^{-1}\left[\frac{1}{p^{10}}\right] - 44L^{-1}\left[\frac{1}{p^{12}}\right]$$

i.e.

$Cx\cos x = 6\,x - 14\frac{x^3}{2!} + 14\frac{x^5}{4!} - 6\frac{x^7}{6!} + 11\frac{x^9}{8!} - 4\frac{y^{11}}{10!}$ which is the same eq$^{\mathbf{n}}$ (2.4)

Containing coefficients as letters in the given plaintext thus we obtained the plaintext

6 14 14 6 11 4

i.e. G O O G L E

Thus the generalized result of example (2.1.1) for decryption is

Theorem 2.1.2: The given cipher text $C_i{}'$ with a given key k_i Can be converted to plain text C_i,under the inverse Laplace transform of $L\{Cx\cos x\} = \sum_{i=0}^{j}\frac{(-1)^i r_i}{p^{2i+2}}$ where $C_i = (-1)^i\left[\frac{26k_i + c_i{}'}{(2i+1)}\right]$ Where $i = 0, 1, 2, 3 \ldots\ldots..$

Case-(ii):

$m = 2 \,\&\, n = 2$

If we take m=2 & n=2 then eq$^{\mathbf{n}}$ (2.2) becomes

$$Cx^2\cos 2x = 6x^2 - 14\frac{2^2x^4}{2!} + 14\frac{2^4x^6}{4!} - 6\frac{2^6x^8}{6!} + 11\frac{2^8x^{10}}{8!} - 4\frac{2^{10}x^{12}}{10!} \tag{2.6}$$

Operating Laplace transform to equation (2.6) we have

$$L[Cx^2\cos 2x] = 6\,L[x^2] - 14\,L\left[\frac{2^2x^4}{2!}\right] + 14L\left[\frac{2^4x^6}{4!}\right] - 6\,L\left[\frac{2^6x^8}{6!}\right] + 11\,L\left[\frac{2^8x^{10}}{8!}\right] - 4\,L\left[\frac{2^{10}x^{12}}{10!}\right]$$

Simplifying the above expression we get

$$L[Cx^2\cos 2x] = \frac{12}{p^3} - \frac{672}{p^5} + \frac{6720}{p^7} - \frac{21504}{p^9} + \frac{253440}{p^{11}} - \frac{540672}{p^{13}} \tag{2,7}$$

AdJusting the resulting values 12,-3072,6720,-21504,253440,-540672 by our method i.e.
12≡ -14mod 26, -3072≡ 4mod 26, 6720≡ 12mod 26, -21504≡ -2mod 26
253440 ≡ 18mod 26, -540672≡ -2mod 26,

Let $C_0{}' = -14$, $C_1{}' = 4$, $C_2{}' = 12$, $C_3{}' = -2$, $C_4{}' = 18$, $C_5{}' = -2$,

The cipher text for given plaintext is given below

14 4 12 2 18 2

To generalize the above result let us assume that $r_0 = 12$, $r_1 = -3072$, $r_2 = 6720$, $r_3 = -21504$, $r_4 = 253440$, $r_5 = -540672$,

By knowing the values of r_i and C_i we have calculated key k_i in tabular form given below

Table-4.4

I	C_i	$r_i = (-1)^i 2^{2i}(2i+1)(2i+2)C_i$	$k_i = \frac{r_i - C'}{26}$	$C_i' = r_i - 26k_i$
0	6	12	1	-14
1	14	-672	-26	4
2	14	6720	258	12
3	6	-21504	827	-2
4	11	253440	9747	18
5	4	-540672	20795	-2

From the above table we see that 1,-26, 258,827,9747,20795 is the required key to crack the original messag
Therefore in general we have

Theorem 2.1.3: Let $C_{0,}C_{1,}C_{2,\dots\dots}$ Cbe coefficients of $x^2 \cos 2x$ then the given plaintext in terms of C_i under the Laplace transform of $C \cos 2x$ can be converted to cipher text $C_i' = r_i - 26k_i$ where $r_i = (-1)^i 2^{2i}(2i+1)(2i+2)C_i$ and key is given by $k_i = \frac{r_i - C_i'}{26}$ for $i = 0,1,2,3,4, \dots \dots ., j$.

By applying I.L.T. to $eq^{\mathbf{n}}(2.7)$ it becomes

$$L^{-1}\{L[Cx^2 \cos 2x]\} = L^{-1}\left[\frac{12}{p^3}\right] - L^{-1}\left[\frac{672}{p^5}\right] + 6720L^{-1}\left[\frac{1}{p^7}\right] - 21504L^{-1}\left[\frac{1}{p^9}\right] + 253440\, L^{-1}\left[\frac{1}{p^{11}}\right] - 540672\, L^{-1}\left[\frac{1}{p^{13}}\right] \text{i.e.}$$

$$Cx^2 \cos 2x = 6x^2 - 14\frac{2^2x^4}{2!} + 14\frac{2^4x^6}{4!} - 6\frac{2^6x^8}{6!} + 11\frac{2^8x^{10}}{8!} - 4\frac{2^{10}x^{12}}{10!}$$

Which is the equation having coefficients as letters in the given plaintext thus we get the plaintext given below

6 14 14 6 11 4 i.e. G O O G L E

Hence in general we have

Theorem 2.1.4: The given cipher text $C_0' C_1' C_2', \cdots\cdots, C_j'$ can be converted to plain text $C_{0,}C_{1,}C_{2,\dots\dots}$ C by taking the inverse Laplace transform. of $L\{Cx^2 \cos 2x\} = \sum_{i=0}^{j} \frac{(-1)^i r_i}{p^{2i+3}}$ where $I_i = (-1)^i \left[\frac{26k_i + C_i'}{2^{2i}(2i+1)(2i+2)}\right]$

Where $i = 0, 1, 2,3 \dots \dots ..$,j by using the above methodology and considering m=1 & n=2 we obtain the

Theorem 2.1.5: generalizations for encryption and decryption stated below.
Let $C_{0,}C_{1,}C_{2,\dots\dots}$ $C_j$be coefficients of $y \cos 2y$ .Then the given plain text in terms of C_i under the L.T. of $Cy \cos 2y$ can be transformed to cipher text $C' = r_i - 26k_i$ where $r_i = (-1)^i 2^{2i}(2i+1)C_i$ and key is given by

$$k_i = \frac{r_i - C_i'}{26} \text{ for } i = 0,1,2,3,4, \dots \dots ., j$$

Theorem 2.1.6: The given cipher text C_i' with a given key k_i Can be converted to plain text $I_i$under the inverse Laplace transform. Of $L[Cx \cos 2x]$ where

$$C_i = (-1)^i \left[\frac{r_i}{2^{2i}(2i+1)}\right] \text{Where } i = 0, 1, 2,3 \dots \dots .., j$$

From the above generalizations G (4.4.1), G (4.4.3), G (4.4.5) and by induction on m & n more generally

Theorem 2.1.7: Let $C_{0,}C_{1,}C_{2,\dots\dots}$ $C_j$be coefficients of $x^m \cos nx$ Then the given plaintext C_i Under the Laplace transform of $Cx^m \cos nx$ can be transformed to cipher text $C_i' = r_i - 26k_i$ wher

$$r_i = (-1)^i n^{2i}(2i+1)(2i+2) \dots \dots ..(2i+m)C_i \text{ and } k_i = \frac{r_i - C_i'}{26} \text{ for } i = 0,1,2,3,4, \dots \dots ., j.$$

Theorem 2.1.8: The given cipher text C_i' with a given key k_i Can be converted to plaintext I_i,under the inverse Laplace transform of $L[Cx^m \cos nx] = \sum_{i=0}^{j} \frac{(-1)^i r_i}{p^{2i+m+1}}$ where

$$H_i = (-1)^i \left[\frac{26k_i + C_i'}{2^{2i}(2i+1)(2i+2)\dots\dots(2i+m)}\right]$$

where $i = 0, 1, 2,3 \dots \dots ..$,j

3 CONCLUSIONS

From the work which we have done in this paper we conclude that we have applied Laplace transform and inverse Laplace transform to trigonometric cosine function successfully for encryption &decryption respectively.

REFRENCES

1. A.D. Poularikas, The Transforms and Applications Hand-book (McGraHill, 2000) Second edition.
2. Widder D.V. 1946. The Laplace transforms, Princeton University press, USA.
3. Jaegar J.C. 1961, An Introduction to the Laplace transformation with Engineering applications, Methuen London.
4. David M. Burton: Elementary number theory, Seventh edition, McGraw Hill Education (India) Private Limited New Delhi.
5. T.H.Barr, Invitation to Cryptography, Prentice Hall, (2002)
6. A.P. Hiwarekar: A new method of Cryptography using Laplace transform of Hyperbolic function, International Journal of Mathematical archive, 2013, 4(2), pp.206-213.
7. G. Naga Lakshmi, B. Ravikuar and A. Chandra Sekher, A Cryptographic Scheme of Laplace transforms, International Journal of Mathematical archive, 2011, pp. 65-70
8. G.R.Blakely, Twenty years of Cryptography in the open literature Security and Privacy, Proceedings of the IEEE Symposium (May 1999), pp.9-12.
9. Poularikas A.D., 1996. The transforms and applications handbook, CRC Press, USA.
10. H.K.Undegaonkar & R.N.Ingle, "Role of Laplace transforms in integral calculus", International Journal of Mathematical Archive-6(7), 2015-p 21-24, ISSN 2229-5046.

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