Secured Communication by Using Laplace Transforms and Cryptography

Hemant Undegaonkar

Associate Professor, Department of Mathematics, Bahirji Smarak Mahavidyalaya, Basmathnagar, Maharashtra, India

Abstract: ***In this paper we will show that how to create secured communication by applying Laplace transform and cryptography. In the first section of the paper, we will consider one plain text (original message) and convert it to text in hidden form i.e. cipher text by applying Laplace transform to trigonometric sine function. In second section we will convert this cipher text to plain text by applying inverse Laplace transform.***

Keywords: Laplace transform, Inverse Laplace transform, Cryptography, Plain text, cipher text, encryption, decryption

1. Introduction

The word Cryptography comes from the Greek word Kryptos which means hidden and graphin means 'to write'. Cryptography is the branch in which we study some techniques to convert our original message to such a message which could not be easily understandable without providing some additional information or formula. Original message which is to be converted to hidden form is called as plain text and the converted form is called s cipher text.

Encryption means the conversion of plain text to cipher text and decryption. means the conversion of cipher text to plain text. After demonetization in 2016 people likes cashless transactions like, Phone pay, Mobile banking, internet banking, etc. Password is necessary to operate all these facilities. In Mathematics there are some integral transforms like Laplace transform, Sumudu transform, Fourier transform,Elzaki transform etc. [1] Integral transforms contributes in the process of encryption and decryption. The main purpose of this paper is to present method to create such a confidential text so that we can create secured communication. Integral transforms play an important role in solving differential and integral equations and also in other engineering sciences. In the process of cryptography there is a contribution of some integral transforms like Laplace transform, Sumudu transform, and Elzaki transform.

There are various kinds of techniques for the process of encryption and decryption found in literature [2], [4],

A new cryptographic scheme was developed by applying L.T. to hyperbolic sine and cosine functions [2], [4]. In this paper we have applied Laplace transform and Inverse Laplace transform to trigonometric cosine function to establish such results regarding encryption decryption.

Some important definitions & theorems

Def.1 [6] In equation (1.1) if $\alpha = 0$ & $k(p, y) = e^{-py}$ then we define Laplace transform of $g(y)$ by

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

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

Def.2 If F(p)is the Laplace transform of $f(z)$ then the inverse Laplace transform of F(p) is $f(z)$ and we write $L^{-1}\{F(p)\} = f\ (z)$.

Def.3: [3] [The relation of congruent modulo m
Let m be a positive integer. Then an integer b is congruent to an integer c modulo n if n divides $b - c$ .If αb is congruent to c modulo m then symbolically we write $b \equiv c(\text{mod } m)$. If b is not congruent to c modulo m then we denote it as $b \not\equiv c(\text{mod } m)$

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

2. Method of Cryptography by Applying L.T. to Trigonometric Cosine Function

In this section we can transfer the given plain text in to such a hidden text which could not be able to crack without key by operating Laplace transforms.

Suppose that we are given A B C D E F G H………….Z. as a plain text. Initially have to give the following allotment to letters in the given plain text.

$A \to 0, B \to 1, C \to 2, D \to 3, E \to 4, F \to 5, G \to 6, H \to 7, I \to 8, J \to 9, K \to 10, L \to 11, M \to 12, N \to 13, O \to 14, P \to 15, Q \to 16, R \to 1 \to 18, T \to 19, U \to 20, V \to 21, W \to 22, X \to 23, Y \to 24, Z \to 25$

In this section we will apply L.T. to trigonometric cosine function for the process of encryption. Also we will transfer cipher text to plaintext by applying inverse laplace transform

Consider the cosine series given by
$\cos ny = 1 - \frac{n^2y^2}{2!} + \frac{n^4y^4}{4!} - \frac{n^6y^6}{6!} + \frac{n^8y^8}{8!} - \frac{n^{10}y^{10}}{10!}$................then we have

$$y^m \cos ny = y^m - \frac{n^2y^{m+2}}{2!} + \frac{n^4y^{n+4}}{4!} - \frac{n^6y^{m+6}}{6!} + \ldots \qquad (2.1)$$

Suppose that $I_0, I_1, I_2, I_3, I_4, I_5, I_6, I_7, \ldots\ldots I_j$ be coefficients of theeq^n (2.1) then we write this new equation as

$$Iy^m \cos nz = I_0 z^m - I_1 \frac{n^2z^{m+2}}{2!} + I_2 \frac{n^4z^{m+4}}{4!} - I_3 \frac{n^6z^{m+6}}{6!} + \ldots \qquad (2.2)$$

Ex. (1): Let us consider the plaintext given by
M A H A R A J and by our allotment be equivalent to
12 0 7 0 17 0 9

Case (i): when m=1& n=1eq^n (2.2) becomes
$Iz \cos z = I_0 z - I_1 \frac{z^3}{2!} + I_2 \frac{z^5}{4!} - I_3 \frac{z^7}{6!} + I_4 \frac{z^9}{8!}$--
$= I_5 \frac{z^{11}}{10!} + \ldots I_6 \frac{z^{13}}{12!}$.............. (2.3)
Let us assume that $I_0 = 12, I_1 = 0, I_2 = 7, I_3 = 0, I_4 = 17, I_5 = 0, I_6 = 9$, be coefficients of the above eq^n

$$\therefore Iy \cos z = 12z - 0\frac{z^3}{2!} + 7\frac{z^5}{4!} - 0\frac{z^7}{6!} + 17\frac{z^9}{8!} - 0\frac{z^{11}}{10!} + 9\frac{z^{13}}{12!} \qquad (2.4)$$

Applying L.T. to the above eq^n it changes to
$L\{Iz \cos y\} = 12L(z) - 0L\left(\frac{z^3}{2!}\right) + 7L\left(\frac{z^5}{4!}\right) - 0L\left(\frac{z^7}{6!}\right) + 17L\left(\frac{z^9}{8!}\right) - 0L\left(\frac{z^{11}}{10!}\right) + 9L\left(\frac{z^{13}}{12!}\right)$ i.e.

$$L\{Iz \cos z\} = \frac{12}{p^2} - \frac{0}{p^4} + \frac{35}{p^6} - \frac{0}{p^8} + \frac{153}{p^{10}} - \frac{0}{p^{12}} + \frac{117}{p^{14}} \qquad (2.4)$$

Suppose that $s_0 = 12,\ s_1 = 0,\ s_2 = 35, s_3 = 0,\ s_4 = 153,\ s_5 = 0,\ \ s_6 = 117,$

Let us determine $I_i{}'$ by method given in section (2)
$12 \equiv -14 \bmod 26$, $0 \equiv 0 \bmod 26$, $35 \equiv 9 \bmod 26$, $0 \equiv 0 \bmod 26$
$153 \equiv -3 \bmod 26$, $0 \equiv 0 \bmod 26$, $117 \equiv 13 \bmod 26$

Let $I_0{}' = -14,\ I_1{}' = 0,\ I_2{}' = 9,\ I_3{}' = 0,\ I_4{}' = -3,\ I_5{}' = 0,\ I_6{}' = 0,\ I_7{}' = 13$

Assuming the values of $I_0{}', I_1{}', I_2{}', \ldots\ldots\ldots, I_{10}{}'$ to be non-negative the given plaintext M A H A R A J is converted to the cipher text
14 0 9 0 3 0 13 i.e.
O A J A D A N

Similarly by selecting different integers for values of m& n in equation 2.2 and continuing the same process using the methodology (2) we obtain the general result given below.

Theorem (1) Let $I_0, I_1, I_2, \ldots\ldots I_j$ be coefficients of $y^m \cos nz$ Then the given plaintext I_i Under the L.T.of $Iz^m \cos nz$ can be transformed to cipher text $I_i{}' = s - 26k_i$ where $s_i = (-1)^i n^{2i}(2i+1)(2i+2)\ldots\ldots(2i+m)I_i$ and $k_i = \frac{r_i - I_i{}'}{26}$ for $i = 0,1,2,3,4,\ldots\ldots, j$.

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

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

Where $i = 0, 1, 2, 3 \ldots\ldots, j$

3. Conclusions

From the above theory part proved it is clear that by applying Laplace transform and its inverse we can obtain different cipher texts for given plain text which cannot be easily cracked without providing some additional information. Thus Laplace transform with cryptography plays an important role in communication security.

Acknowledgements
I am thankful to the principal Dr. M. M. Jadhav Dr. R. N. Ingle & Dr. P. G. Gawali for providing me some local facilities.

References

[1] G. K. Watugala, Sumudu transforms: a new integral transform to solve differential equations and control engineering problems, International Journal of Mathematical Education in Science and Technology 24(1993), vol. no 1, 35-43.
[2] 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
[3] David M. Burton: Elementary number theory, Seventh edition, McGraw Hill Education (India) Private Limited New Delhi.
[4] G. Naga Lakshmi, B. Ravikuar and A. Chandra Sekher, A Cryptographic Scheme of Laplace transforms, International Journal of Mathematical archive, 2011, pp. 65-70
[5] G.A.Dhanorkar and A.P.Hiwarekar, A generalized Hill ciphers using Matrix transformation international Journal of Math.Sci and Engineering applications, Vol.5.no. 4(July 2011). pp. 19-23.
[6] Poularikas A.D., 1996. The transforms and applications handbook, CRC Press, USA.
[7] Jaegar J.C. 1961, An Introduction to the Laplace transformation with Engineering applications, Methuen London.
[8] Asiru M.A., Further properties and its applications, Int.Journal of Mathematical education in science and Technology, 33(3), pp. 441-449.