Role of Some Integral Transforms in Cryptography

Hemant K. Undegaonkar, R. N. Ingle

Abstract: There are so many methods for the process of cryptography in literature. In this paper we present encryption and decryption method by using Laplace transform & Sumudu transform and their inverses. The purpose of using this method is for more security in communication as compared to other methods because cipher text obtained by this method could not be cracked by other persons easily. In the first part we apply Laplace transform to trigonometric cosine function for Sumudu transform for the same purpose. Finally we conclude by comparing these two methods.

Key-words: Laplace transform, Sumudu transform, Inverse Laplace transform, Inverse Sumudu transform, Cryptography, Encryption, Decryption.

I. INTRODUCTION

Cryptography is the science of making communications unintelligible to all except authorized parties. Classically the making and breaking of secret codes has usually been confined to diplomatic and military practices. With the growing quantity of digital data stored and communicated by electronics data-processing systems, organizations in both the public and commercial sectors have felt the need to protect information from unwanted intrusion. In the language of cryptography codes are called ciphers and the information to be concealed is called plaintext. Transformed message in secret form is called ciphertext. The process of converting from plaintext to cipher text is said to be encrypting whereas the process of changing from cipher text to plaintext is said to be decrypting. The word Cryptography comes from the Greek word kryptos which means hidden and graphem means “to write”.

After demonetization in 2016 people prefers cashless transactions like A.T.M., Pay TM, Mobile banking, internet banking etc. to operate these facilities password is required. Cryptology consists of Cryptography and cryptanalysis which deals with breaking secret messages.

In Mathematical Sciences a transformation is such a device which is useful for the conversion of one function \( f(t) \) into another function of new variables \( f(p) \) and \( f(s) \) etc. For almost two centuries we have used integral transforms successfully in Mathematical sciences and Engineering field. Some authors have applied Sumudu transform to exponential functions in the process of encryption and decryption [6]. In this paper we are applying Sumudu transform to trigonometric cosine functions for the same process. 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].

A. Laplace transforms [1, 2]

Def. 1 The Laplace transform of \( g(y) \) is defined by

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

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

Def. 2 If \( F(p) \) is the Laplace transform of \( g(y) \) then the inverse Laplace transform of \( F(p) \) is \( g(y) \) and we write \( \mathcal{L}^{-1}[F(p)] = g(y) \).

B. Sumudu transforms [3]

In 1990 Gamage K. Watugala has introduced a new transform namely Sumudu transform which is similar to Laplace transform [3]. The meaning of Sumudu is smooth and this is Sinhala word. Sumudu transform is theoretical dual of the Laplace transform.

Def. 3 The sumudu transform of \( f(x) \) is defined by

\[
G(u) = \sum_{x} f(x) u^{-x} \text{ over the set B of functions defined by}
\]

\[
B = \{ f(x) \text{ such that } \exists \, N \in \mathbb{R} : x_1, x_2 > 0, |f(x)| < Ne^{\lambda x}, x \in (0, N) \}
\]

Def. 4 If \( G(u) \) is the Sumudu transform of \( f(x) \) then the inverse Sumudu transform of \( G(u) \) is \( f(x) \) and we write \( S^{-1}[G(u)] = f(x) \).

II. METHOD OF CRYPTOGRAPHY BY APPLYING L.T. TO TRIGONOMETRIC SINE & COSINE FUNCTION [6, 7]

In this method we can convert the given plain text in to such a hidden text which could not possible 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. In the first step we have to give the following allotment to letters in the given plain text.

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

Consider the trigonometric Cosine series given by

\[
y^m \cos ny = y^m - \frac{n^2 y^{m+2}}{2!} + \frac{n^4 y^{m+4}}{4!} - \ldots \ldots \ldots (1)
\]

Let \( H_0 \), \( H_1 \), \( H_2 \), …… \( H_l \) be the coefficients of the \( eq \n \)

\[
H_y^m \cos ny = H_0 y^m + H_1 \frac{n^2 y^{m+2}}{2!} + H_2 \frac{n^4 y^{m+4}}{4!} - \ldots \ldots \ldots (2)
\]
By operating Laplace transform to eqn \(2\) we will obtain one equation containing some new variable in denominator and some values in the numerator (we call them as resulting values say \(r_i\)) adjusting these resulting values such that \(r_i \equiv H_i \mod 26\) for \(i = 0,1, \cdots , j\) we obtain \(H_i\) which is our required cipher text.

As decryption is the reverse process of encryption we can obtain plain text by applying I.L.T. of \(L[H_y^m \cos ny]\).

To determine cipher text by applying L.T. to trigonometric function we may use the above method by considering some series of the form \(H_y^m \cos ny\)

III. ENCRYPTION & DECRYPTION OF GIVEN MESSAGE BY APPLYING LAPLACE TRANSFORM & INVERSE LAPLACE TRANSFORM

Ex. (3.1): consider the plaintext given by

\[
\begin{array}{cccccccccc}
P & A & T & A & L & G & A & N & G & A
\end{array}
\]

and by our allotment be equivalent to

\[
\begin{array}{cccccccccc}
15 & 0 & 19 & 0 & 11 & 6 & 0 & 13 & 6 & 0
\end{array}
\]

Let us assume that \(H_0 = 15, H_1 = 0, H_2 = 19, H_3 = 0, H_4 = 11, H_5 = 6, H_6 = 0, H_7 = 13, H_8 = 6, H_9 = 0\)

Case (i): when \(m = 1\) & \(n = 1\) eqn \(2\) becomes

\[
H_y \cos y = H_0 y - H_1 \frac{y^3}{2!} + H_2 \frac{y^5}{4!} - H_3 \frac{y^7}{6!} + H_4 \frac{y^9}{8!} + \cdots
\]

\[
15 y - 0 \frac{y^3}{2!} + 19 \frac{y^5}{4!} - 0 \frac{y^7}{6!} + 11 \frac{y^9}{8!} + 6 \frac{y^{11}}{10!} + \cdots
\]

Operating Laplace transform to both sides of equation (3) we have

\[
L[H_y \cos y] = 15 L[y] - 0 \frac{y^2}{2!} + 19 \frac{y^4}{4!} - 0 \frac{y^6}{6!} + 11 \frac{y^8}{8!} + 6 \frac{y^{10}}{10!} + \cdots
\]

\[
L[y^9] - \frac{6}{10} L[y^{11}] + \frac{0}{12} L[y^{13}] - \frac{13}{14} L[y^{15}] + \frac{6}{16} L[y^{17}] - \frac{9}{18} L[y^{19}] + \cdots
\]

\[
L[H_y \cos y] = \frac{15}{y^2} - \frac{0}{y^4} + \frac{95}{y^6} - \frac{0}{y^8} + \frac{99}{y^{10}} - \frac{66}{y^{12}} + \frac{0}{y^{14}} - \frac{195}{y^{16}} + \cdots
\]

\[
= \frac{102}{y^{18}} - \frac{0}{y^{20}}
\]

Let \(r_0 = 15, r_1 = 0, r_2 = 95, r_3 = 0, r_4 = 99, r_5 = -66, r_6 = 0, r_7 = -195, r_8 = 102, r_9 = 0\)

Let us calculate \(H_i\) such that \(r_i \equiv H_i \mod 26\)

\[
H_0 \equiv -11, H_1 \equiv 0
\]

\[
H_2 = 17, H_3 = 0, H_4 = -5, H_5 = 12, H_6 = 0, H_7 = 13, H_8 = -2, H_9 = 0
\]

Thus cipher text for given plaintext will be

\[
\begin{array}{cccccccccc}
11 & 0 & 17 & 0 & 5 & 12 & 0 & 13 & 2 & 0
\end{array}
\]

\[\text{i.e.} \ 15 \equiv -11 \mod 26, 0 \equiv 0 \mod 26, 95 \equiv 17 \mod 26, 0 \equiv 0 \mod 26, 99 \equiv -5 \mod 26, -66 \equiv 12 \mod 26, \text{ etc.}
\]

Let \(H_i = -11, H_i = 0,\)

\[
H_2 = 17, H_3 = 0, H_4 = -5, H_5 = 12, H_6 = 0, H_7 = 13, H_8 = -2, H_9 = 0
\]

From the above table we see that \(1,0,3,0,4,-3,0,-8,4,0\) is the key to open the given message which is in hidden form. we may generalize this the result as

\[R(1): \text{Let } H_0, H_1, H_2, \ldots , H_n \text{ be coefficients of } y \cos y \text{ then the given plaintext in terms of } H_n \text{ under the Laplace transform of } H_y \cos y \text{ can be converted to cipher text } H_i = r_i - 26k_i \text{ where } r_i = (-1)^{(2i + 1)}H_i \text{ and } k_i = \frac{r_i - H_i}{26} \text{ for } i = 0, 1, 2, 3, 4, \ldots , j.
\]

Similarly by operating Laplace transform to equation (2) for the values \(2,3, \ldots \) for \(m\) & \(n\) more generally we have

Table 1: Representing encryption process by applying Laplace transforms

| i | \(H_i\) | \(r_i = (-1)^i(2i + 1)H_i\) | \(k_i = \frac{r_i - H_i}{26}\) | \(H_i = r_i - 26k_i\) |
|---|---|---|---|---|
| 0 | 15 | 15 | 1 | -11 |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 19 | 95 | 3 | 17 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 11 | 99 | 4 | -5 |
| 5 | 6 | -66 | -3 | 12 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 13 | -195 | -8 | 13 |
| 8 | 6 | 102 | 4 | -2 |
| 9 | 0 | 0 | 0 | 0 |
R (2): Let $H_0, H_1, H_2, \ldots H_i$ be coefficients of $y^m \cos y$ then the given plaintext in terms of $H_i$ under the Laplace transform of $y^m \cos y$ can be converted to cipher text $H_i$.

$$k_i = \frac{r_i - H_i}{26}$$ for $i = 0, 1, 2, 3, \ldots, j$.

$$L^{-1}[L\{H_i \cos y\}] = L^{-1}\left[\frac{15}{x^2}\right] - L^{-1}\left[\frac{0.1}{x^3}\right] + L^{-1}\left[\frac{95}{x^6}\right] - L^{-1}\left[\frac{90}{x^7}\right] + L^{-1}\left[\frac{8}{x^{11}}\right] - L^{-1}\left[\frac{14}{x^{12}}\right] - L^{-1}\left[\frac{14}{x^{13}}\right] + L^{-1}\left[\frac{14}{x^{14}}\right]$$

Hence, we have

$$\cos y = 15y^2 - 20y^3 + 19y^4 - 10y^5 + 6y^6 - 3y^7 + 0y^8 + 11y^9$$

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

15 0 19 0 11 6 0 13 6 0 i.e. P A T A L G A N A

Thus we may generalize the result for decryption given below

R (3): The given cipher text $l_i$ with a given key $k_i$ Can be converted to plaintext $l_j$ under the inverse Laplace transform of $L[y^m \cos ny] = \sum_{i=0}^{j} (-1)^{i}k_i$ where

$$H_i = (-1)^i \left(\frac{26k_i + H_i}{2i+1}\right)$$

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

IV. ENCRYPTION & DECRYPTION OF GIVEN MESSAGE BY APPLYING SUMUĐU TRANSFORM & INVERSE SUMUĐU TRANSFORM

By applying Sumudu transform to equation (3) we have

$$S[\cos y] = 15S[y^2] - \frac{20}{12}S[y^3] + \frac{19}{14}S[y^4] - \frac{10}{16}S[y^5] + \frac{95}{18}S[y^6]$$

Therefore

$$S[\cos y] = 15u^2 - \frac{20}{12}u^3 + \frac{19}{14}u^4 - \frac{10}{16}u^5 + \frac{95}{18}u^6$$

Let $r_8=30, r_1 = 0, r_2 = 9120, r_3 = 0, r_4 = 253440, r_5 = -811008, r_6 = 0, r_7 = -51118080, r_8 = 120324096, r_9 = 0$

Let us calculate $H_i$ such that $r_i = H_i \pmod{26}$ i.e. 30 \equiv 4 \mod{26}, 0 \equiv 0 \mod{26}, 9120 \equiv 20 \mod{26}, 0 \equiv 0 \mod{26}, 253440 \equiv 18 \mod{26}, -811008 \equiv -16 \mod{26}, 0 \equiv 0 \mod{26}, -51118080 \equiv 0 \mod{26}, 120324096 \equiv 22 \mod{26}, 0 \equiv -20 \mod{26}

Let $H_0, H_1, \ldots = 0, H_2 = 20, H_3 = 0, H_4 = -18, H_5 = -16, H_6 = 0, H_7 = 0, H_8 = 22, H_9 = 0$. Thus cipher text for given plaintext will be

$$4 0 20 0 -18 -16 0 0 22 0 0 i.e.$$
Table(2): Representing encryption process by applying Sumudu transforms

| i | \( H_i \) | \( r_i = (-1)^i2^{3i}(2i+1)(2i+2)H_i \) | \( k_i = \frac{r_i - H_i'}{26} \) | \( H_i' = r_i - 26k_i \) |
|---|---|---|---|---|
| 0 | 15 | 30 | 1 | 4 |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 19 | 9120 | 350 | 20 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 11 | 253440 | 9747 | 18 |
| 5 | 6 | \(-811008\) | 31192 | \(-16\) |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 13 | \(-5111808\) | 1966080 | 0 |
| 8 | 6 | 120324096 | 4627849 | 22 |
| 9 | 0 | 0 | 0 | 0 |

From the above table (2) we see that 1,0,350,0,9747,31192,0,1966080,4627849,0 is the key to open the given message which is in hidden form. We may generalize the result for encryption given below.

**G(4):** Let \( H_0,H_1,H_2,H_3,\ldots\ldots,H_J \) be coefficients of \( y^2 \cos 2y \) then the given plaintext in terms of \( H_i \) under the Sumudu transform of \( H \) \( y^2 \cos 2y \) can be converted to cipher text \( H_i' = r_i - 26k_i \) Where

\[
r_i = (-1)^i2^{3i}(2i+1)(2i+2)H_i \quad \text{and key is given by}
\]

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

Similarly by operating Laplace transform to equation (2.2) for the values 3, 4,.... for \( m \) & \( n \) more generally we have

**G(5):** Let \( H_0,H_1,H_2,H_3,\ldots\ldots,H_J \) be coefficients of \( y^m \cos ny \) then the given plaintext in terms of \( H_i \) under the Sumudu transform of \( H \) \( y^m \cos ny \) can be converted to cipher text \( H_i' = r_i - 26k_i \) Where

\[
r_i = (-1)^i2^{3i}(2i+1)(2i+2)\cdots\cdots(2i+m)H_i \quad \text{and key is given by}
\]

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

**VI. CONCLUSION**

Firstly we conclude that Laplace transform & Sumudu transform plays an important role in the process of cryptography i.e. encryption & decryption. Applying both transforms for the same plain text to the same function we will get the same cipher text but applying both transforms to different functions we can obtain different cipher texts for the same plain text.

**VII. FUTURE SCOPE**

Now a day’s online banking, online purchasing, etc plays an important role in daily life. For operating these online facilities password is required for confidentiality. Also in military services, Indian police services at every stage confidentiality are required. Thus cryptography is very useful field and there is scope for research in future

**VIII. ACKNOWLEDGEMENT**

I am very thankful to research centre N.E.S.Science college Nanded for providing facilities of library. I am also thankful to our institute Bahirji Smarak Mahavidyalaya Basmathnagar Dist.Hingoli for support.

**REFERENCES**

1. Alexander Stanoyevitch, Introduction to cryptography with Mathematical foundation and computer implementations, CRC Press, (2002).
2. A.D. Poularikas, The Transforms and Applications Hand-book (McGraHill, 2000)
3. A.P. Hiwarekar: A new method of Cryptography using Laplace transform of Hyperbolic function
4. Belgacem,F.B.M. Boundary value problems with indefinite weight and applications, International Journal of problems of non linear Analysis in Engineering systems,10(2) (1999),pp.51-58.Second edition.
5. David M. Burton: Elementary number theory, Seventh edition, McGraw Hill Education (India) Private Limited New Delhi.
6. D.S.Bodke and S.K.Panchal,” Use of Sumudu transform in Cryptography”, Bulletin of the Marathwada Mathematical Society, Vol.16, no.1, June 2015, pp.1-
7. F.B.M. Belgacem and A.A.Karaballi, Sumudu Transform Fundamental Properties Investigations and Applications, Journal of Applied Mathematics and Stochastic Analysis, Vol.2006, Article ID 91083, Pages 1-23
8. G. Naga Lakshmi, B. Ravikuar and A. Chandra Sekher, A Cryptographic Scheme of Laplace transforms, International Journal of Mathematical archive, 2011, pp. 65-70
9. [9] 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.
10. [10] Johannes A. Buchmann, Introduction to Cryptography, Fourth Edition, Indian Reprint, Springer, (2009).
11. [11] Stallings W.: Cryptography and Network Security, fourth edition, entice Hall, 2005.
12. [12] Sumudu transforms a new integral transform to solve differential equations and control engineering problems, Mathematical Engineering in Industry 6(1998), no. 319-329
13. [13] T.H.Barr, Invitation to Cryptography, Prentice Hall, (2002)
14. [14] Widder D.V. 1946. The Laplace transforms, Princeton University press, USA.

AUTHORS PROFILE

Dr. Hemant K. Undegaonkar: He is working as Assistant Professor in Department of Mathematics at Bahirji Smarak Mahavidyalaya, Basmathnagar since 1996. His research area is integral transforms and their applications. He is a member of Marathwada Mathematical Society, Aurangabad.

Dr. R. N. Ingle: He is working as Principal at Mathematics at Bahirji Smarak Mahavidyalaya, Basmathnagar. He is research Supervisor in S.R.T.M. University Nanded.