



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 graphein 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 $f(p), f(s)$ 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].

Revised Manuscript Received on February 05, 2020.

* Correspondence Author

Dr. Hemant K. Undegaonkar, Department of Mathematics, Bahirji Smarak Mahavidyalaya, Basmathnagar, Hingoli (Maharashtra) India.

E-mail: hemantundegaonkar@gmail.com

Dr. R. N. Ingle, Principal, Bahirji Smarak Mahavidyalaya, Basmathnagar, Hingoli (Maharashtra) India.

E-mail: Ingleraju11@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

A. Laplace transforms [1, 2]

Def. 1 The Laplace transform of $g(y)$ is defined 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 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 $L^{-1}\{F(p)\} = g(y)$.

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 $G(u) = \int_0^{\infty} \frac{1}{u} e^{-\frac{x}{u}} f(x) dx$ over the set B of functions defined by

$$B = \{f(x) \text{ such that } \exists N, x_1, x_2 > 0, |f(x)| < N e^{\frac{|x|}{x_1}}, x \in (-1)^j X[0, \infty)\}$$

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 → 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 → 1 → 18, T → 19, U → 20, V → 21, W → 22, X → 23, Y → 24, Z → 25

Consider the trigonometric Cosine series given by

$$y^m \cos ny = y^m - \frac{n^2 y^{m+2}}{2!} + \frac{n^4 y^{m+4}}{4!} - \dots \quad (1)$$

Let $H_0, H_1, H_2, \dots, H_j$ be the coefficients of the eqⁿ

∴ We write

$$Hy^m \cos ny = H_0 y^m - H_1 \frac{n^2 y^{m+2}}{2!} + H_2 \frac{n^4 y^{m+4}}{4!} - \dots \quad (2)$$



Role of Some Integral Transforms in Cryptography

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 ≡ H_i' mod 26 for i = 0,1,⋯,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{Hy^m cos ny}.

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

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

Ex. (3.1): consider the plaintext given by

P A T A L G A N G A and by our allotment be equivalent to

15 0 19 0 11 6 0 13 6 0

Let us assume that H₀ = 15, H₁ = 0, H₂ = 19, H₃ = 0, H₄ = 11, H₅ = 6, H₆ = 0, H₇ = 13, H₈ = 6, H₉ = 0

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

$$Hy \cos y = H_0 y - H_1 \frac{y^3}{2!} + H_2 \frac{y^5}{4!} - H_3 \frac{y^7}{6!} + H_4 \frac{y^9}{8!} \dots (3)$$

$$\therefore Hy \cos y = 15y - 0 \frac{y^3}{2!} + 19 \frac{y^5}{4!} - 0 \frac{y^7}{6!} + 11 \frac{y^9}{8!} - 6 \frac{y^{11}}{10!} + 0 \frac{y^{13}}{12!} - 13 \frac{y^{15}}{14!} + 6 \frac{y^{17}}{16!} - 0 \frac{y^{19}}{18!}$$

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

$$L\{Hy \cos y\} = 15 L[y] - \frac{0}{12} L[y^3] + \frac{19}{14} L[y^5] - \frac{0}{16} L[y^7] + \frac{11}{18} L[y^9] - \frac{6}{110} L[y^{11}] + \frac{0}{112} L[y^{13}] - \frac{13}{114} L[y^{15}] + \frac{6}{116} L[y^{17}] - \frac{0}{118} L[y^{19}]$$

$$L\{Hy \cos y\} = \frac{15}{s^2} - \frac{0}{s^4} + \frac{95}{s^6} - \frac{0}{s^8} + \frac{99}{s^{10}} - \frac{66}{s^{12}} + \frac{0}{s^{14}} - \frac{195}{s^{16}} + \frac{102}{s^{18}} - \frac{0}{s^{20}} \quad (4)$$

Let r₀=15, r₁ = 0, r₂ = 95, r₃ = 0, r₄ = 99, r₅ = -66, r₆ = 0, r₇ = -195, r₈ = 102, r₉ = 0

Let us calculate H_i' such that r_i ≡ H_i' mod 26

i.e.

15 ≡ -11 mod 26, 0 ≡ 0 mod 26, 95 ≡ 17 mod 26, 0 ≡ 0 mod 26, 99 ≡ -5 mod 26, -66 ≡ 12 mod 26, 0 ≡ 0 mod 26, -195 ≡ 13 mod 26, 102 ≡ -2 mod 26, 0 ≡ -0 mod 26

Let H₀' = -11, H₁' = 0,

H₂' = 17, H₃' = 0, H₄' = -5, H₅' = 12, H₆' = 0, H₇' = 13, H₈' = -2,

H₉' = 0 Thus cipher text for given plaintext will be

11 0 17 0 5 12 0 0 13 2 0 i.e.

L A R A F M A N C A

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

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 the this result as

R(1): Let H₀, H₁, H₂,..... H_j be coefficients of y cos y then the given plaintext in terms of H_i under the Laplace transform of Hy cos y can be converted to cipher text H_i' = r_i - 26k_i where r_i = (-1)ⁱ(2i + 1)H_i and

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

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

R(2): Let $H_0, H_1, H_2, \dots, H_j$ be coefficients of $y^m \cos n y$ then the given plaintext in terms of H_i under the Laplace transform of $y^m \cos n y$ can be converted to cipher text H_i' where $r_i = (-1)^{in^{2i}}(2i + 1)(2i + 2) \dots (2i + m)$ &

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

$$L^{-1}\{L\{Hy \cos y\}\} = L^{-1}\left[\frac{15}{s^2}\right] - L^{-1}\left[\frac{0}{s^4}\right] + L^{-1}\left[\frac{95}{s^6}\right] - L^{-1}\left[\frac{0}{s^8}\right] + L^{-1}\left[\frac{99}{s^{10}}\right] - L^{-1}\left[\frac{66}{s^{12}}\right] + L^{-1}\left[\frac{0}{s^{14}}\right] - L^{-1}\left[\frac{195}{s^{16}}\right] + L^{-1}\left[\frac{102}{s^{18}}\right] - L^{-1}\left[\frac{0}{s^{20}}\right]$$

$$Hy \cos y = 15y - 0\frac{y^3}{2!} + 19\frac{y^5}{4!} - 0\frac{y^7}{6!} + 11\frac{y^9}{8!} - 6\frac{y^{11}}{10!} + 0\frac{y^{13}}{12!} - 13\frac{y^{15}}{14!} + 6\frac{y^{17}}{16!} - 0\frac{y^{19}}{18!}$$

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 G A

Thus we may generalize the result for decryption given below

R(3): 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 $L\{I_i^m \cos ny\} = \sum_{i=0}^j \frac{(-1)^i r_i}{p^{2i+m+1}}$ where

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

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

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

By applying Sumudu transform to equation (3) we have

$$S\{Hy \cos y\} = 15 S[y] - \frac{0}{12} S[y^3] + \frac{19}{14} S[y^5] - \frac{0}{16} S[y^7] + \frac{11}{18} S[y^9] - \frac{6}{110} S[y^{11}] + \frac{0}{112} S[y^{13}] - \frac{13}{114} S[y^{15}] + \frac{6}{116} S[y^{17}]$$

$$= 15!1 u - 0!3 u^3 + \frac{19}{14}!5 u^5 - \frac{0}{16}!7 u^7 + \frac{11}{18}!9 u^9 - \frac{6}{110}!11 u^{11} + \frac{0}{112}!13 u^{13} - \frac{13}{114}!15 u^{15} + \frac{6}{116}!17 u^{17} - \frac{0}{118}!19 u^{19}$$

Therefore $S\{Hy \cos y\} = 15u - 0u^3 + 95u^5 - 0u^7 + 99u^9 - 66u^{11} + 0u^{13} - 182u^{15} + 102u^{17} - 0u^{19}$

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

Here we obtained the same values of r_i by applying Sumudu transform to the same function which implies that we obtain the same cipher text for given plain text by applying Laplace transform and Sumudu transform in this case.

By taking $m=n=2$ equation (2) becomes

$$Hy^2 \cos 2y = H_0 y^2 - H_1 \frac{2^2 y^4}{!2} + H_2 \frac{2^4 y^6}{!4} - H_3 \frac{2^6 y^8}{!6} + H_4 \frac{2^8 y^{10}}{!8} - H_5 \frac{2^{10} y^{12}}{!10} + H_6 \frac{2^{12} y^{14}}{!12} - H_7 \frac{2^{14} y^{16}}{!14} + H_8 \frac{2^{16} y^{18}}{!16} - H_9 \frac{2^{18} y^{20}}{!18}$$

i.e. we have

$$Hy^2 \cos 2y = 15y^2 - 0\frac{2^2 y^4}{!2} + 19\frac{2^4 y^6}{!4} - 0\frac{2^6 y^8}{!6} + 11\frac{2^8 y^{10}}{!8} - 6\frac{2^{10} y^{12}}{!10} + 0\frac{2^{12} y^{14}}{!12} - 13\frac{2^{14} y^{16}}{!14} + 6\frac{2^{16} y^{18}}{!16} - 0\frac{2^{18} y^{20}}{!18} \quad (5)$$

Applying Sumudu transform to equation (5) we obtain

$$S\{Hy^2 \cos 2y\} = 15 S[y^2] - 0 S\left[\frac{2^2 y^4}{!2}\right] + 19 S\left[\frac{2^4 y^6}{!4}\right] - 0 S\left[\frac{2^6 y^8}{!6}\right] + 11 S\left[\frac{2^8 y^{10}}{!8}\right] - 6 S\left[\frac{2^{10} y^{12}}{!10}\right] + 0 S\left[\frac{2^{12} y^{14}}{!12}\right] - 13 S\left[\frac{2^{14} y^{16}}{!14}\right] + 6 S\left[\frac{2^{16} y^{18}}{!16}\right] - 0 S\left[\frac{2^{18} y^{20}}{!18}\right]$$

$$S\{Hy^2 \cos 2y\} = 15!2 u^2 - 0!4 u^4 + 19\frac{2^4}{!4}!6 u^6 - 0!8 u^8 + 11\frac{2^8}{!8}!10 u^{10} - 6\frac{2^{10}}{!10}!12 u^{12} + 0!14 u^{14} - 13\frac{2^{14}}{!14}!16 u^{16} + 6\frac{2^{16}}{!16}!18 u^{18} - 0!20 u^{20}$$

Therefore we have

$$S\{Hy^2 \cos 2y\} = 30u^2 - 0u^4 + 9120u^6 - 0u^8 + 253440u^{10} - 811008u^{12} + 0u^{14} - 51118080u^{16} + 120324096u^{18} - 0u^{20}$$

Let $r_0=30, r_1 = 0, r_2 = 9120, r_3 = 0, r_4 = 253440, r_5 = -811008, r_6 = 0, r_7 = -51118080, r_8 = 120324096, r_9 = 0$

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

Let $H_0'=4, H_1'=0, H_2'=20, H_3'=0, H_4'=-18, H_5'=-16, H_6'=0, H_7'=0, H_8'=22, H_9'=0$ Thus cipher text for given plaintext will be

4 0 20 0 -18 -16 0 0 22 0 i.e. E A U A S Q A A W A



Table(2): Representing encryption process by applying Sumudu transforms

i	H _i	r _i = (-1) ⁱ 2 ²ⁱ (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	-51118080	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 H₀,H₁,H₂,H₃,.....,H_j be coefficients of y² cos 2y then the given plaintext in terms of H_i under the Sumudu transform of H y² cos 2y

Can be converted to cipher text H_i' = r_i - 26k_i Where
 r_i = (-1)ⁱ2²ⁱ(2i + 1)(2i + 2)H_i and key is given by
 k_i = $\frac{r_i - H_i'}{26}$ for i = 0,1,2,3,4,,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 H₀,H₁,H₂,H₃,.....,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)ⁱ2²ⁱ(2i + 1)(2i + 2) (2i + m)H_i and key is given by
 k_i = $\frac{r_i - H_i'}{26}$ for i = 0,1,2,3,4,,j

V. RESULTS AND DISCUSSION

In the first part by applying Laplace transform to equation (2) we obtained cipher text L A R A F M A N C A for the plain text P A T A L G A N G A But by applying Sumudu transform to the same function we obtained the same cipher text .It means to obtain different cipher texts for plain text we have to apply integral transform to different functions. in second part by applying Sumudu transform to new function we obtained new cipher text E A U A S Q A A W.

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.Bodkhe 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.