# Application of Laplace Transform For Cryptographic Scheme

A.P.Hiwarekar *

**ABSTRACT -** Information protection has been an important part of human life from ancient time. In computer society, information security becomes more and more important for humanity and new emerging technologies are developing in an endless stream. Cryptography is one of the most important technique used for securing transmission of messages and protection of data. Examples includes, e-commerce; electronic communications such as mobile communications, sending private emails; business transactions; Pay-TV; transmitting financial information; security of ATM cards; computer passwords etc, which touches on many aspects of our daily lives. Cryptography provide privacy and security for the secret information by hiding it. It is done through mathematical technique.

In this paper we developed a new mathematical method for cryptography, in which we used Laplace transform for encrypting the plain text and corresponding inverse Laplace transform for decryption. This paper is based on the work of [7,9,10].

***Key words:*** *Cryptography, Data encryption, Applications to coding theory and cryptography, Algebraic coding theory; cryptography, Laplace Transforms.*

***Mathematics Subject classification***: [94A60, 68P25,14G50, 11T71, 44A10]

*Vidya Pratishthan's College of Engineering, Vidyanagari, M.I.D.C. Baramati, Dist. Pune-413133, M.S., India. & Email: hiwarekaranil@gmail.com

## 1 INTRODUCTION

When we send a message to someone, we always suspect that someone else will intercept it and read it or modify it before re-sending. There is always a desire to know about a secret message being sent or received between two parties with or without any personal, financial or political gains. It is no wonder that to have the desire to send a message to someone so that nobody else can interpret it. Thus information security has become a very critical aspect of modern computing system. Information security is mostly achieved through the use of cryptography.

Various techniques for cryptography are found in literature [1],[2],[3],[5],[11],[16],[17]. Mathematical technique using matrices for the same are found in Dhanorkar and Hiwarekar,[4]; Overbey, Traves and Wojdylo,[13]; Saeednia,[15]. In Naga Lakshmi, Ravi Kumar and Chandra Sekhar,[7]; Hiwarekar,[9] and [10]; they encrypt a string by using series expansion of $f(t)$ and its Laplace transform. Here in this paper we use hyperbolic cosine functions.

## 2 DEFINITIONS AND STANDARD RESULTS:

**Definition 2.1.:** Plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

**Definition 2.2.:** When plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

**Definition 2.3.:** Encryption transforms a plain text message into cipher text, whereas decryption transforms a cipher text message back into plain text.

Every encryption and decryption process has two aspects: The algorithm and the key. The key is used for encryption and decryption that makes the process of cryptography secure. Here we require following results.

**2.1. The Laplace Transform:** If $f(t)$ is a function defined for all positive values of $t$, then the Laplace transform of $f(t)$ is defined as

$$L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)dt, \quad (1)$$

provided that the integral exists. Here the parameter $s$ is a real or complex number. The corresponding inverse Laplace transform is

$$L^{-1}\{F(s)\} = f(t), \quad (2)$$

[6],[8],[12],[14].

**Theorem 2.1** *Laplace transform is a linear transform. That is, if*

$$\begin{aligned} &L\{f_1(t)\} = F_1(s), L\{f_2(t)\} = F_2(s), \cdots, \\ &L\{f_n(t)\} = F_n(s), \end{aligned} \quad (3)$$

*then*

$$\begin{aligned} &L\{c_1 f_1(t) + c_2 f_2(t) \cdots + c_n f_n(t)\} \\ &= c_1 F_1(s) + c_2 F_2(s) + \cdots + c_n F_n(s), \end{aligned} \quad (4)$$

*where* $c_1$ , $c_2, \cdots, c_n$ *are constants, [6,8,12,14].*

**2.3. STANDARD RESULTS ON LAPLACE TRANSFORMS:** Laplace transform has many applications in various fields [6],[8],[12],[14] such as Mechanics, Electrical circuit, Beam problems, Heat conduction, Wave equation, Transmission lines, Signals and systems, Control systems, Communication systems, Hydrodynamics, Solar systems.

We require the following standard results of Laplace transform :

$$L\{\cosh kt\} = \frac{s}{s^2 - k^2}, \quad s \geq |k|, \quad (5)$$

$$L^{-1}\{\frac{s}{s^2 - k^2}\} = \cosh kt, \quad (6)$$

$$L\{t^n\} = \frac{n!}{s^{n+1}}, \quad n \in N, \quad (7)$$

$$L^{-1}\{\frac{n!}{s^{n+1}}\} = t^n, \quad (8)$$

$$L\{t^n e^{kt}\} = \frac{n!}{(s-k)^{n+1}}, \quad (9)$$

$$L^{-1}\{\frac{n!}{(s-k)^{n+1}}\} = t^n e^{kt}, \quad (10)$$

where $n = 0, 1, 2, 3, \cdots$, the positive integers, [6],[8],[12],[14].

# 3 MAIN RESULTS

## 3.1 ENCRYPTION

We consider standard expansion

$$\begin{aligned} t\cosh rt =& t + \frac{r^2 t^3}{2!} + \frac{r^4 t^5}{4!} + \frac{r^6 t^7}{6!} \\ &+ \cdots + \frac{r^{2n} t^{2n+1}}{2n!} + \cdots \\ &= \sum_{i=0}^{\infty} \frac{r^{2i} t^{2i+1}}{2i!}, \end{aligned} \quad (11)$$

where $r \in N$ is a constant with $N$ is the set of natural numbers. We allocated 0 to A and 1 to B then Z will be 25. Let given message plain text string be 'PROFESSOR'. It is equivalent to

15 17 14 5 4 18 18 14 17.

. We assume that

$G_0 = 15$, $G_1 = 17$, $G_2 = 14$,
$G_3 = 5$, $G_4 = 4$, $G_5 = 18$,
$G_6 = 18$, $G_7 = 14$, $G_8 = 17$,
$G'_n = 0$ for n $\geq 9$.

ISBN: 978-988-19251-0-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Let us consider

$$\begin{aligned}
f(t) &= Gt\cosh 2t \\
&= t\Big\{G_0.1 + G_1\frac{2^2t^2}{2!} + G_2\frac{2^4t^4}{4!} \\
&+ G_3\frac{2^6t^6}{6!} + G_4\frac{2^8t^8}{8!} + G_5\frac{2^{10}t^{10}}{10!} \\
&+ G_6\frac{2^{12}t^{12}}{12!} + G_7\frac{2^{14}t^{14}}{14!} + G_8\frac{2^{16}t^{16}}{16!}\Big\} \\
&= 15t + 17\frac{2^2t^3}{2!} + 14\frac{2^4t^5}{4!} + 5\frac{2^6t^7}{6!} + 4\frac{2^8t^9}{8!} \\
&+18\frac{2^{10}t^{11}}{10!} + 18\frac{2^{12}t^{13}}{12!} + 14\frac{2^{14}t^{15}}{14!} + 17\frac{2^{16}t^{17}}{16!} \\
&= \sum_{i=0}^{\infty}\frac{G_i 2^{2i}t^{2i+1}}{2i!}.
\end{aligned}$$

Taking Laplace transform on both sides we have

$$\begin{aligned}
L\{f(t)\} &= L\{Gt\cosh 2t\} = L\Big\{5t + 17\frac{2^2t^3}{2!} \\
&+14\frac{2^4t^5}{4!} + 5\frac{2^6t^7}{6!} + 4\frac{2^8t^9}{8!} + 18\frac{2^{10}t^{11}}{10!} \\
&+18\frac{2^{12}t^{13}}{12!} + 14\frac{2^{14}t^{15}}{14!} + 17\frac{2^{16}t^{17}}{16!}\Big\} \\
&= \frac{15}{s^2} + \frac{204}{s^4} + \frac{1120}{s^6} + \frac{2240}{s^8} + \frac{9216}{s^{10}} + \\
&\frac{202752}{s^{12}} + \frac{958464}{s^{14}} + \frac{3440640}{s^{16}} + \frac{18939904}{s^{18}}.
\end{aligned}$$

Adjusting resultant values

15 204 1120 2240 9216 202752 958464 3440640 18939904

to mod 26 the given plain text string gets converts to cipher text string

15 22 2 4 12 4 0 8 22.

Hence the given message string 'PROFESSOR' get converted to 'PWCEMEAIW'.

with key $k_i$ for $i = 0, 1, 2, 3, \cdots$, as

$$0 \quad 7 \quad 43 \quad 86 \quad 354$$
$$7798 \quad 36864 \quad 132332 \quad 728457. \qquad (12)$$

These results can be generalized in the form of the following theorem

**Theorem 3.1** *The given plain text string in terms of $G_i, i = 1, 2, 3\cdots$, under Laplace transform of $Gt\cosh rt$, (that is by writing them as a coefficient of $t\cosh rt$, and then taking Laplace transform) can be converted to cipher text $G'_i$, where*

$$G'_i = q_i - 26k_i, \quad for \quad i = 0, 1, 2, 3, \cdots, \qquad (13)$$

*and*

$$q_i = r^{2i}(2i+1)G_i \quad for\ i = 0, 1, 2, 3, \cdots, \quad r = 1, 2, 3, \cdots, \qquad (14)$$

*with key*

$$k_i = \frac{q_i - G'_i}{26} \quad for\ i = 0, 1, 2, 3, \cdots. \qquad (15)$$

### 3.2 DECRYPTION

We assume that the received message string be 'PWCEMEAIW' which is equivalent to

15 22 2 4 12 4 0 8 22.

Assuming

$G'_0 = 15$, $G'_1 = 22$, $G'_2 = 2$, $G'_3 = 4$, $G'_4 = 12$, $G'_5 = 4$, $G'_6 = 0$, $G'_7 = 8$, $G'_8 = 22$, $G'_n = 0$ for $n \geq 9$.

The given key $k_i$ for $i = 0, 1, 2, 3, \cdots$, as

$$0 \quad 7 \quad 43 \quad 86 \quad 354$$
$$7798 \quad 36864 \quad 132332 \quad 728457. \qquad (16)$$

Let

$$q_i = 26k_i + G'_i \quad for\ i = 0, 1, 2, 3, \cdots. \qquad (17)$$

Hence we have $q_i$ *for* $i = 0, 1, 2, 3, \cdots, 8$, are respectively given by

15 204 1120 2240 9216 202752 958464 3440640 18939904.

We consider

$$G\{\frac{-d}{ds}\}\frac{1}{(s^2-2^2)} = \sum_{i=0}^{\infty}\frac{q_i}{s^{2i+2}} = \frac{15}{s^2} + \frac{204}{s^4} + \frac{1120}{s^6} + \frac{2240}{s^8} + \frac{9216}{s^{10}} + \frac{202752}{s^{12}} + \frac{958464}{s^{14}} + \frac{3440640}{s^{16}} + \frac{18939904}{s^{18}}.$$

Taking inverse Laplace transform we get

$$\begin{aligned}
Gt\cosh 2t &= 15t + 17\frac{2^2t^3}{2!} + 14\frac{2^4t^5}{4!} + 5\frac{2^6t^7}{6!} + 4\frac{2^8t^9}{8!} \\
&+18\frac{2^{10}t^{11}}{10!} + 18\frac{2^{12}t^{13}}{12!} + 14\frac{2^{14}t^{15}}{14!} + 17\frac{2^{16}t^{17}}{16!}.
\end{aligned}$$

ISBN: 978-988-19251-0-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Hence we have

$G_0 = 15,\quad G_1= 17,\ G_2= 14, G_3= 5, G_4= 4,$

$G_5= 18,\ G_6= 18, G_7= 14,\ G_8= 17,$

$G_n= 0$ for n $\geq 9$.

Which is equivalent to 'PROFESSOR'.
These results can be obtained in the form of the following theorem

**Theorem 3.2** *The given cipher text string in terms of $G_i, i = 1, 2, 3\cdots$, with given key $k_i$ for $i = 0, 1, 2, 3, \cdots$, under inverse Laplace transform of*

$$G\{\frac{-d}{ds}\}\frac{1}{(s^2-r^2)}=\sum_{i=0}^{\infty}\frac{q_i}{s^{2i+2}}.$$

*can be converted to plain text $G_i$, where*

$$G_i = \frac{26k_i + G'_i}{r^{2i}\,(2i+1)},\quad i = 0, 1, 2\cdots, \tag{18}$$

*and*

$$q_i\ = 26k_i + G'_i \quad for\ i = 0, 1, 2, 3, \cdots. \tag{19}$$

# 4 GENERALIZATION

We now extend the results obtained in section 3 for more generalized functions. Here we are assuming that $N$ is a set of natural numbers. For encryption of the given message string in terms of $G_i$. We consider

$$f(t) = Gt^j \cosh rt,$$
$$r, j \in\ N(the\ set\ of\ Natural\ numbers). \tag{20}$$

We follow the procedure as discussed in section 3. Hence taking Laplace transform of $f(t)$ we can convert given message string $G_i$ to $G'_i$, where

$$G'_i = G_i r^{2i}(2i+1)(2i+2)\cdots (2i+j)\ mod\ 26 = q_i\ mod\ 26, \tag{21}$$

where

$$q_i = G_i r^{2i}(2i+1)(2i+2)\cdots(2i+j),\quad i = 0, 1, 2, 3, \cdots, \tag{22}$$

with key

$$k_i\ = \frac{q_i - G'_i}{26}\quad for\ i = 0, 1, 2, 3, \cdots. \tag{23}$$

For decryption of a received message string in terms of $G'_i$ we consider

$$G\{\frac{-d}{ds}\}^j\frac{1}{(s^2-r^2)}=\sum_{i=0}^{\infty}\frac{q_i}{s^{2i+j+1}}.$$

Taking inverse Laplace transform and using procedure discussed in section 3, we can convert given message string $G'_i$ to $G_i$ where

$$G_i = \frac{26k_i+G'_i}{r^{2i}(2i+1)(2i+2)\cdots(2i+j)},\quad i = 0, 1, 2\cdots. \tag{24}$$

These results can be generalized in the form of the following theorems

**Theorem 4.1** *The given plain text string in terms of $G_i, i = 1, 2, 3\cdots$, under Laplace transform of $Gt^j \cosh rt$, (that is by writing them as a coefficient of $t^j \cosh rt$, and then taking Laplace transform) can be converted to cipher text $G'_i$, where*

$$G'_i = q_i - 26k_i,\quad for\ for\ i = 0, 1, 2, 3, \cdots, \tag{25}$$

*and*

$$q_i = G_i r^{2i}(2i+1)(2i+2)\cdots(2i+j),\quad i = 0, 1, 2, 3, \cdots, \tag{26}$$

*with key $k_i$ given by (23).*

**Theorem 4.2** *The given cipher text string in terms of $G_i, i = 1, 2, 3\cdots$, with given key $k_i$ for $i = 0, 1, 2, 3, \cdots$, under inverse Laplace transform of*

$$G\{\frac{-d}{ds}\}^j\frac{1}{(s^2-r^2)}=\sum_{i=0}^{\infty}\frac{q_i}{s^{2i+j+1}}.$$

*can be converted to plain text $G_i$, where*

$$G_i = \frac{26k_i+G'_i}{r^{2i}(2i+1)(2i+2)\cdots(2i+j)},\quad i = 0, 1, 2\cdots, \tag{27}$$

*and*

$$q_i\ = 26k_i + G'_i\quad for\ i = 0, 1, 2, 3, \cdots. \tag{28}$$

The method developed in this paper can be used in the form of following algorithm.

ISBN: 978-988-19251-0-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

**4.1 ENCRYPTION ALGORITHM:**

1) Treat every letter in the plain text message as a number, so that A=0, B=1, C=2,....,Z=25.
2)The plain text message $Gi$ is organized as a finite sequence of numbers, based on the above conversion. Only consider $Gi$ till the length of input string, i.e. i=0 to n-1.
3) Consider suitable function $f(t)$ given by equation (20).Take Laplace transform and get formula (21) for encryption. Hence each character in the input string converts to new position $G'i$.
4) Key value for each character can be obtained by equation (23).
5) Send $G'i$ and $Ki$ as pair to receiver.
On similar way we can obtain decryption algorithm.

# 5 ILLUSTRATIVE EXAMPLES

Suppose the original message be string 'PROFESSOR'.Using our results of section 4.2,we can convert it to

1. 'PBSRKKAYD' for $r = 5, j = 1$,
2. 'EQMUQEACG' for $r = 3, j = 2$,
3. 'EOKUOMASS' for $r = 4, j = 2$,
4. 'MSSYYAAUE' for $r = 4, j = 3$,
5. 'WKQGSAAQG' for $r = 1, j = 4$.

**DISCUSSION AND CONCLUDING REMARKS**

1. We used the long key,for example, key of 256 bit, to break it by Bruce force attack,when faster super computer are used, it requires about $3.31 \times 10^{56}$ years, which is almost impossible. Here for faster super computer, (as per wikipedia) 10.51 pentaflops = $10.51 \times 10^{15}$flops.

2. Many sectors such as banking and other financial institutions are adopting e-services and improving their internet services. However, the e-service requirements are also opening up new opportunity to commit financial fraud. Internet banking fraud is one of the most serious electronic crimes (e-crimes) and mostly committed by unauthorized users. The new method of key generation scheme developed in this paper may be used for a fraud prevention mechanism.

3. In the proposed work we develop a new cryptographic scheme using Laplace transforms of hyperbolic functions and the key is the number of multiples of mod n. Therefore it is very difficult for an eyedropper to trace the key by any attack.

4. In a two- party communication between entities A and B, sound cryptographic practice dictates that the key be kept changing frequently for each communication session. The results in section 4 provide as many transformations as per the requirements which is the most useful factor for changing key.

5. The similar results can be obtained by using Laplace transform of some other suitable functions. Hence extension of this work is possible.

*ACKNOWLEDGEMENT*

Author is thankful to Principal Dr.S.B.Deosarkar and Vidya Pratishthan's College of Engineering, Baramati, Dist. Pune, Maharashtra, India,for the support to this work. Auther is also thankful to BCUD University of Pune,India for the financial support to this work under research project 'Better network security using generalised Hill cipher algoritham'.

# References

[1] **Alexander Stanoyevitch**, Introduction to cyrptography with mathematical foundations and computer implementations,CRC Press, (2002).

[2] **Barr T.H.**, Invitation to Cryptography, Prentice Hall, (2002).

[3] **Blakley G.R.**, Twenty years of Cryptography in the open literature, Security and Privacy 1999, Proceedings of the IEEE Symposium, 9-12, (May 1999).

[4] **Dhanorkar G.A. and Hiwarekar A.P.**, A generalized Hill cipher using matrix transformation, International J. of Math. Sci. & Engg. Appls,Vol. 5 No. IV, 19-23, (July 2011).

[5] **Eric C., Ronald K., James W.C.**, Netwark Security Bible Second edn.,Wiley India pub.(2009).

[6] **Erwin Kreyszing**, Advanced Engineering Mathematics,John Wiley and Sons Inc.(1999).

[7] **G.Naga Lakshmi, B.Ravi Kumar and A.Chandra Sekhar**, A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2, 2515-2519, (2011).

[8] **Grewal B.S.**, Higher Engineering Mathematics, Khanna Pub., Delhi, (2005).

[9] **Hiwarekar A.P.**, A new method of cryptography using Laplace transform,International Journal of Mathematical Archive,3(3),1193-1197,(2012).

[10] **Hiwarekar A.P.**, A new method of cryptography using Laplace transform of hyperbolic functions,International Journal of Mathematical Archive,4(2),208-213,(2013).

[11] **Johannes A. Buchmann**, Introduction to Cryptography,Fourth Edn.,Indian Reprint ,Springer,(2009).

[12] **Lokenath Debnath, Dambaru Bhatta**, Integrl Transforms and Their Applications,Chapman and Hall/CRC,First Indian edn.(2010).

[13] **Overbey J., Traves W.and Wojdylo J.**, On the Keyspace of the Hill Cipher,

Cryptologia, 29, 59-72, (January 2005).

[14] **Ramana B.V.**, Higher Engineering Mathematics, Tata McGraw-Hills, (2007).

[15] **Saeednia S.**, How to Make the Hill Cipher Secure, Cryptologia, 24, 353-360, (October 2000).

[16] **Stallings W.**, Cryptography and network security, 4th edition, Prentice Hall, (2005).

[17] **Stallings W.**, Network security essentials: Applications and standards, first edition, Pearson Education, Asia, (2001).

ISBN: 978-988-19251-0-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)