

APPLICATION OF LAPLACE - MELLIN TRANSFORM FOR CRYPTOGRAPHY

*Mampi Saha

ABSTRACT

Every living thing needs protection. In India, we are facing various types of crimes. Among which, cyber crime is becoming very challenging task all over the world. Many software companies make various application to protect our data or information from hackers. According to a survey, there were around 13,301 cases of cyber crime reported in the country but in 2015 we already have over 3,00,000 cases and it's increasing 300% in 3 years. So, it is very important to secure the internet and other form of electronic communications such as sending private emails, mobile communications, Pay-TV, transmitting financial information, security of ATM cards, computer passwords etc, which touches on many aspects of our daily lives. In this paper, we discuss the application of Laplace - Mellin transformation for cryptography.

Keywords: Cryptography, Data encryption, Applications to coding theory and cryptography, Algebraic coding theory, Laplace - Mellin transforms

1. INTRODUCTION

'Cryptography is the art of achieving security by enclosing messages to make them non – readable'. Some common terms belonging to the process of Cryptography are as below:

- *Plain text:* The original message, which written by user.
- *Cipher text:* It is the coding form of plaintext.
- *Encryption:* The process of obscuring information to make it unreadable without special knowledge.
- *Decryption:* The process of converting cipher text into plaintext.
- *Cryptography:* The art of devising the cipher.

2. DEFINITION

2.1 Laplace Transformation: The Laplace Transformation has a long history of development. It is defined by the Pierre Simmon Marquis De Laplace. The Laplace Transformation is very effective device in Mathematic, Physics and other branches of science which is used to solving problem.

Let $f(l)$ be the function of variable l , $0 < l < \infty$. Laplace Transformation is defined as:

$$\mathcal{L} [f(l)] = F(s) = \int_0^{\infty} e^{-sl} f(l) dl \quad (1.1)$$

*Department of Mathematics, Ranchi University, Ranchi, Jharkhand

where, e^{-sl} is Kernel of the Laplace Transformation .Where s is the parameter, $s > 0$. The inverse of Laplace Transformation is defined by $\mathcal{L}^{-1}\{F(s)\}$

$$\mathcal{L}^{-1}\{F(s)\} = f(l) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} e^{sl} F(s) ds \quad (1.2)$$

2.2 Mellin Transformation: This Transformation was introduced first time when Riemann studied famous Zeta function. But R.H Mellin gave its systematic formulation of the transformation. Also he developed its theories and field of application.

Let $f(m)$ be any function defined on variable, where m belongs $0 \leq m < \infty$. The Mellin Transformation is defined as

$$\mathfrak{M} [f(m)] = F(p) = \int_0^{\infty} m^{p-1} f(m) dm \quad (1.3)$$

where, m^{p-1} is Kernel of the Transformation of Mellin Transformation; p is the parameter, $p > 0$. The inverse of Mellin Transformation is defined by $\mathfrak{M}^{-1}\{F(p)\}$

$$\mathfrak{M}^{-1}\{F(p)\} = f(m) = \frac{1}{2\pi i} \int_{b-i\infty}^{b+i\infty} m^{-p} F(p) dp \quad (1.4)$$

2.3 Some Results for Laplace and Mellin Transform

1. $\mathcal{L} [l^n] = \frac{\Gamma(n+1)}{s^{n+1}}$ and $\mathcal{L}^{-1} \left\{ \frac{\Gamma(n+1)}{s^{n+1}} \right\} = l^n$
2. $\mathfrak{M} [e^{-m^2}] = \frac{1}{2} \Gamma \left(\frac{p}{2} \right)$ and $\mathfrak{M}^{-1} \left\{ \frac{1}{2} \Gamma \left(\frac{p}{2} \right) \right\} = e^{-m^2}$

3. MAIN RESULTS

3.1 Encryption

We consider standard expansion

$$\begin{aligned} \operatorname{sech} rl &= 1 - \frac{(rl)^2}{\Gamma 2} + 5 \frac{(rl)^4}{\Gamma 4} - 61 \frac{(rl)^6}{\Gamma 6} + \dots \dots \dots \\ &= \frac{E_0(rl)^0}{\Gamma 1} + \frac{E_2(rl)^2}{\Gamma 3} + \frac{E_4(rl)^4}{\Gamma 5} + \frac{E_6(rl)^6}{\Gamma 7} + \dots \dots \dots = \sum_{n=0}^{\infty} \frac{E_{2n}(rl)^{2n}}{\Gamma(2n+1)} \end{aligned}$$

Where, $r \in 2N$ is a constant and E_{2n} is an Euler number, we take $r = 4$.

$$E_{2n} = i \sum_{k=1}^{2n+1} \sum_{j=0}^k \binom{k}{j} \frac{(-1)^j (k-2j)^{2n+1}}{2^k i^k k}$$

$$E_{10} = 10! \left(-\frac{1}{10!} + \frac{2}{2!8!} + \frac{2}{4!6!} - \frac{3}{2!^2 6!} - \frac{3}{2!4!^2} + \frac{4}{2!^3 4!} - \frac{1}{2!^5} \right)$$

$$= 9! \left(-\frac{1}{9!} + \frac{3}{1!^2 7!} + \frac{6}{1!3!5!} + \frac{1}{3!^3} - \frac{5}{1!^4 5!} - \frac{10}{1!^3 3!^2} + \frac{7}{1!^6 3!} - \frac{1}{1!^9} \right) = -50521$$

E_0	=	1
E_2	=	-1
E_4	=	5
E_6	=	-61
E_8	=	1385
E_{10}	=	-50521
E_{12}	=	2702765
E_{14}	=	-199360981
E_{16}	=	19391512145
E_{18}	=	-2404879675441

We allocated 0 to 'a' and 1 to 'b' then 'z' will be 25, A to Z take 26 to 51, Space bar takes code 52, and last number 0 to 9 takes 53 to 62. Now we start coding, let given message 'E Crime16'. First convert it in secret code, like

$$C_0 = E = 30, \quad C_1 = \text{Spacebar} = 52, \quad C_2 = C = 28, \quad C_3 = r = 17, \quad C_4 = i = 8,$$

$$C_5 = m = 12, \quad C_6 = e = 4, \quad C_7 = 1 = 54, \quad C_8 = 6 = 59, \quad C_n = 0, n \geq 8$$

We take function as:

$$f(l, m) = C_n \operatorname{sech} rl e^{-m^2} = \sum_{n=0}^{\infty} \frac{E_{2n}(rl)^{2n}}{\Gamma(2n+1)} C_n e^{-m^2}$$

First, take Laplace - Mellin Transform both sides:

$$\mathfrak{L}\mathfrak{M} [f(l, m)] = F(s, p) = \int_0^{\infty} \int_0^{\infty} e^{-sl} m^{p-1} \sum_{n=0}^{\infty} \frac{E_{2n}(rl)^{2n}}{\Gamma(2n+1)} C_n e^{-m^2} dl dm$$

$$F(s, p) = \int_0^{\infty} \sum_{n=0}^{\infty} \frac{E_{2n}(rl)^{2n}}{\Gamma(2n+1)} C_n e^{-sl} dl \int_0^{\infty} m^{p-1} e^{-m^2} dm$$

$$\mathfrak{L}\mathfrak{M} [f(l, m)] = \mathfrak{L} \left\{ \sum_{n=0}^i \frac{E_{2n}(rl)^{2n}}{\Gamma(2n+1)} C_n \right\} \frac{1}{2} \Gamma\left(\frac{p}{2}\right)$$

$$\mathfrak{L}\mathfrak{M} [f(l, m)] = \mathfrak{L} \left\{ \frac{E_0 C_0 (rl)^0}{\Gamma 1} + \frac{E_2 C_1 (rl)^2}{\Gamma 3} + \frac{E_4 C_2 (rl)^4}{\Gamma 5} + \frac{E_6 C_3 (rl)^6}{\Gamma 7} + \dots \dots \dots \right\} \frac{1}{2} \Gamma\left(\frac{p}{2}\right)$$

$$= \frac{1}{2} \Gamma\left(\frac{p}{2}\right) \left\{ 30 \frac{E_0 \Gamma_1}{s \Gamma_1} + 52 \frac{E_2(4)^2 \Gamma_3}{s^3 \Gamma_3} + 28 \frac{E_4(4)^4 \Gamma_5}{s^5 \Gamma_5} + 17 \frac{E_6(4)^6 \Gamma_7}{s^7 \Gamma_7} + 8 \frac{E_8(4)^8 \Gamma_9}{s^9 \Gamma_9} + 12 \frac{E_{10}(4)^{10} \Gamma_{11}}{s^{11} \Gamma_{11}} \right. \\ \left. + 4 \frac{E_{12}(4)^{12} \Gamma_{13}}{s^{13} \Gamma_{13}} + 54 \frac{E_{14}(4)^{14} \Gamma_{15}}{s^{15} \Gamma_{15}} + 59 \frac{E_{16}(4)^{16} \Gamma_{17}}{s^{17} \Gamma_{17}} \right\} \quad (1.5)$$

$$= \Gamma\left(\frac{p}{2}\right) \left\{ 15 \frac{E_0}{s} + 26 * 16 \frac{E_2}{s^3} + 14 * 256 \frac{E_4}{s^5} + 17 * 2048 \frac{E_6}{s^7} + 4 * 65536 \frac{E_8}{s^9} + 6 * 1048576 \frac{E_{10}}{s^{11}} + 2 \right. \\ \left. * 16777216 \frac{E_{12}}{s^{13}} + 27 * 268435456 \frac{E_{14}}{s^{15}} + 59 * 2147483648 \frac{E_{16}}{s^{17}} \right\}$$

$$= \Gamma\left(\frac{p}{2}\right) \left\{ \frac{15}{s} + \frac{416}{s^3} + \frac{17920}{s^5} + \frac{2123776}{s^7} + \frac{363069440}{s^9} + \frac{3.1785e + 011}{s^{11}} + \frac{9.0689e + 013}{s^{13}} \right. \\ \left. + \frac{1.4449e + 018}{s^{15}} + \frac{2.4569e + 021}{s^{17}} \right\} \quad (1.6)$$

Where,

$h_0 = 15,$	$h_1 = 416,$	$h_2 = 17920$
$h_3 = 2123776,$	$h_4 = 363069440,$	$h_5 = 317850648576,$
$h_6 = 90689744404480,$	$h_7 = 1.4449e + 018,$	$h_8 = 2.4569e + 021$

We assume q_n and t_n the quotient and remainder of the term of above series , where $n=1,2,3,\dots$

$h_n = 63q_n + t_n$	where $t_n = C'_n$	
$q_0 = 0,$	$q_1 = 6,$	$q_2 = 284,$
$q_3 = 33710,$	$q_4 = 5763006,$	$q_5 = 5.0452e + 09$
$q_6 = 1.4395e + 01,$	$q_7 = 2.2935e + 016,$	$q_8 = 3.8999e + 019$

So, code states be change in

$$C'_0 = 15, C'_1 = -38, C'_2 = 28, C'_3 = -46, C'_4 = 62, C'_5 = -6, C'_6 = 4, C'_7 = -54, C'_8 = 23, \\ C'_n = 0 \text{ as } n > 8$$

Put the value of Euler number, calculated all value and at last take mod 63 with all entries.

$$= \Gamma\left(\frac{p}{2}\right) \left\{ \frac{15}{s} - \frac{38}{s^3} + \frac{28}{s^5} - \frac{46}{s^7} + \frac{62}{s^9} - \frac{6}{s^{11}} + \frac{4}{s^{13}} - \frac{54}{s^{15}} + \frac{23}{s^{17}} \right\} \quad (1.7)$$

We changed all remainder to positive:

$$= \Gamma\left(\frac{p}{2}\right) \left\{ \frac{15}{s} + \frac{25}{s^3} + \frac{28}{s^5} + \frac{17}{s^7} + \frac{62}{s^9} + \frac{57}{s^{11}} + \frac{4}{s^{13}} + \frac{9}{s^{15}} + \frac{23}{s^{17}} \right\} \quad (1.8)$$

Hence the message 'E Crime16' converted into 'pzCr94ejx'.

THEOREM 1.1: " C_n " is the term of plaintext for $n = 0,1,2, \dots$, it convert into cipher text " C'_n " with keys q_n , for $n = 0,1,2, \dots$ by using Laplace- Mellin transform.

The function which we take,

$$f(l, m) = C_n \operatorname{sech} rl e^{-m^2}$$

Where
$$h_n = \frac{1}{2} E_{2n}(4)^{2n} C_n$$

$$C'_n = h_n - 63q_n \quad \text{for } n = 0,1,2, \dots \quad \text{and} \quad \frac{h_n - C'_n}{63} = q_n$$

3.2 Decryption

We have received message as 'pzCr94ejx' which is equivalent to

$$15 \quad 25 \quad 28 \quad 17 \quad 62 \quad 57 \quad 4 \quad 9 \quad 23$$

Our assumption function is of Euler numbers (it's is alternative series), so we should change 2nd, 4th, 6th and 8th terms to negative, then we get-

$$15 \quad -38 \quad 28 \quad -46 \quad 62 \quad -6 \quad 4 \quad -54 \quad 23$$

$$f(s, p) = \Gamma\left(\frac{p}{2}\right) \sum_{n=0}^i \frac{h_n}{s^{2n-1}}$$

$$= \Gamma\left(\frac{p}{2}\right) \left\{ \frac{15}{s} + \frac{416}{s^3} + \frac{17920}{s^5} + \frac{2123776}{s^7} + \frac{363069440}{s^9} + \frac{3.1785e + 011}{s^{11}} + \frac{9.0689e + 013}{s^{13}} \right.$$

$$\left. + \frac{1.4449e + 018}{s^{15}} + \frac{2.4569e + 021}{s^{17}} \right\}$$

We take inverse Laplace – Mellin Transform (first, we take inverse Laplace transform and after reducing equation we again take inverse Mellin transform), then above equation become

$$f(l, m) = C_n \operatorname{sech} rl e^{-m^2} = \sum_{n=0}^{\infty} \frac{E_{2n}(rl)^{2n}}{\Gamma(2n + 1)} C_n e^{-m^2}$$

Hence the message change cipher text to plain text.

THEOREM 1.2: " C'_n " is the term of cipher text for $n = 0,1,2, \dots$, it convert into plain text " C_n " with keys h_n , for $n = 0,1,2, \dots$ by using Laplace- Mellin transform.

The function which we take
$$f(s, p) = \Gamma\left(\frac{p}{2}\right) \sum_{n=0}^i \frac{h_n}{s^{2n-1}}$$

Where

$$C_n = 2 \frac{(63q_n + t_n)}{E_{2n}(4)^{2n}} \quad \text{and} \quad h_n = C'_n + 63q_n \quad \text{for } n = 0,1,2, \dots$$

4. CONCLUSION

In the proposed work, a new cryptographic scheme has been introduced using Laplace-Mellin transform 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.

REFERENCES

1. Barr T.H. – *Invitation to Cryptography*, Prentice Hall, 2002.
2. Blakley G.R. – *Twenty years of Cryptography in the open literature*, Security and Privacy May 1999, Proceedings of the IEEE Symposium, 9-12.
3. Debnath L, Bhatta D. *Integral Transforms and Their Applications*, Chapman and Hall/CRC, First Indian edn., 2010.
4. G. Naga Lakshmi, Ravi Kumar B. and Chandra Sekhar A. – *A cryptographic scheme of Laplace transforms*, International Journal of Mathematical Archive-2(12), 2011, 2515-2519.
5. Hiwarekar A.P.- *A new method of Cryptography using Laplace transform*, International Journal of Mathematical Archive-2(12), 2012, 1193-1197.
6. Hiwarekar AP. *A new method of cryptography using Laplace transform of hyperbolic functions*, International Journal of Mathematical Archive 2013; 4(2): 208-213.
7. Hiwarekar AP. *Application of Laplace Transform for Cryptographic Scheme*. Proceeding of World Congress on Engineering 2013; II, LNCS, 95-100.
8. Hiwarekar AP. *New Mathematical Modeling for Cryptography*. Journal of Information Assurance and Security, MIR Lab USA, 2014; 9: 027-033.
9. Overbey J, Traves W, Wojdylo J. *On the Keyspace of the Hill Cipher*, Cryptologia, 2005; 29: 59-72.
10. Ramana BV. *Higher Engineering Mathematics*, Tata McGraw-Hills, 2007.
11. Saeednia S. *How to Make the Hill Cipher Secure*. Cryptologia 2000; 24: 353-360.
12. Stallings W. *Cryptography and network security*, 4th edition, Prentice Hall, 2005.
13. Stallings W. *Network security essentials: Applications and standards*, first edition, Pearson Education, Asia, 2001.
14. Stanoyevitch A. *Introduction to cryptography with mathematical foundations and computer implementations*, CRC Press, 2002.
15. Sudhir K. Pundir and Rimple – *Theory of Numbers*, Pragati Prakashd, 2006.