International Journal of Mathematical Archive-8(7), 2017, 143-146
Available online through www.ijma.info ISSN 2229 – 5046

APPLICATION OF LAPLACE - MELLIN TRANSFORM TO CRYPTOGRAPHY

Dr. M. M. P. SINGH[1], Mrs. MAMPI SAHA*[2]

**[1]Professor, [2]Research Scholar, University Department of Mathematics,
Basic Science Building Ranchi University Ranchi, Morabadi-834008, Jharkhand, India.**

(Received On: 19-06-17; Revised & Accepted On: 27-07-17)

ABSTRACT

In today's India, we are facing various types of crimes. Out of these crimes, protection against cybercrime is very challenging task. Many software companies make various applications to protect sensible data or information from hackers.

According to a report, there were around 13,301 cases of cyber crime reported in the country in 2011, but we already have over 3, 00,000 cases reported in 2015. Hence it has incased by a huge 2155% in 4 years. So it is very important to secure internet communication, internet transactions, mobile communications, mobile phone transactions, Pay–TV, transmitting financial information, security of ATM cards, computer passwords etc, which touches on many aspects of our daily lives.

In this section, we will discuss the application of Laplace-Mellin transformation for cryptography [4], [5] [6].

Key words: *Cryptography, Data encryption, Applications to coding theory and cryptography, Algebraic coding theory, Laplace - Mellin transforms.*

Mathematics Subject classification: *94A60, 68P25, 14G50, 11T71, 44A30.*

1. INTRODUCTION

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

a. Plain text: The original message, which written by user.
b. Cipher text: It is the coding form of plaintext.
c. Encryption: The process of obscuring information to make it unreadable without special knowledge.
d. Decryption: The process of converting cipher text into plaintext.
e. Cryptography: The art of devising the cipher.
f. Cryptology: The cryptography and cryptanalyst is together are called cryptology.

2. DEFINATION

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

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

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

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

Corresponding Author: Mrs. Mampi Saha,
Research Scholar, University Department of Mathematics,
Basic Science Building Ranchi University Ranchi, Morabadi-834008, Jharkhand, India.*

2.2 Mellin Transformation: This Transformation is introduced first time when Riemann studied famous Zeta function. But R.H Mellin give 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

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

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

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

2.3 SOME RESUTL FOR LAPLACE AND MELLIN TRANSFORM

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

3. MAIN RESULTS

3.1 Encryption: We consider standard expansion

$$\operatorname{sech} rl = \frac{E_0(rl)^0}{\Gamma 1} + \frac{E_2(rl)^2}{\Gamma 3} + \frac{E_4(rl)^4}{\Gamma 5} + \frac{E_6(rl)^6}{\Gamma 7} + \cdots \ldots \ldots \ldots = \sum_{n=0}^{\infty} \frac{E_{2n}(rl)^{2n}}{\Gamma(2\mathrm{n}+1)}$$

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

$C_0 = E = 30,\ \ C_1 = Spacebar = 52,\ \ \ C_2 = C = 28,\ \ C_3 = r = 17,\ \ \ C_4 = i = 8,$
$C_5 = m = 12,\ \ C_6 = e = 4,\ \ C_7 = 1 = 54,\ \ C_8 = 6 = 59,\ \ \ C_n = 0, n \geq 8$

We take function as

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

First take Laplace - Mellin Transform both side

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

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

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

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

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

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

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

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 reminder of the term of above series , where n=1,2,3,….

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

So, code states be change in

$C_0^{'} = 15\ ,\ C_1^{'} = -38, C_2^{'} = 28, C_3^{'} = -46, C_4^{'} = 62, C_5^{'} = -6, C_6^{'} = 4, C_7^{'} = -54\ , C_8^{'} = 23, \qquad C_n^{'} = 0\ as\ n > 8$

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 change 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 massage ‘E Crime16’ converted into ‘pzCr94ejx’.

Theorem 1.1: "C_n" is the term of plaintext for $n = 0,1,2, \ldots \ldots$, it convert into cipher text "$C_n^{'}$" with keys q_n, for $n = 0,1,2, \ldots \ldots$ by using Laplace- Mellin transform.

The function which we take, $f(l,m) = C_n\ \operatorname{sech} rl\ \ e^{-m^2}$
where $h_n = \frac{1}{2}E_{2n}(4)^{2n}\, C_n$

$C_n^{'} = \ h_n - 63q_n \quad for\ n = 0,1,2, \ldots \ldots \ and\ \ \frac{h_n - C_n^{'}}{63} = q_n$

3.2 Decryption

We have received message as ‘pzCr94ejx’ which is equivalent to

15 25 28 17 62 57 4 9 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

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

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

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

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 $n = 0,1,2, \ldots \ldots$, it convert into plain text "C_n" with keys h_n, for $n = 0,1,2, \ldots \ldots$ 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

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

4. CONCLUDING

In the proposed work a new cryptographic scheme is introduced using Laplace-Mellin transforms 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.

5. 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. Integrl Transforms and Their Applications, Chapman and Hall/CRC, First Indianedn., 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 cyrptography with mathematical foundations and computer implementations, CRC Press, 2002.
15. Sudhir K. Pundir and Rimple – Theory of Numbers, Pragati Prakashed, 2006.

Source of support: Nil, Conflict of interest: None Declared.