International Journal of Mathematical Archive-3(3), 2012, Page: 1193-1197
Available online through www.ijma.info ISSN 2229 – 5046

A NEW METHOD OF CRYPTOGRAPHY USING LAPLACE TRANSFORM

A. P. Hiwarekar*

Vidya Pratishthan's College of Engineering, Vidyanagari, M.I.D.C. Baramati, Dist.Pune, Maharashtra, Pin- 413133, India

E-mail: anilhiwarekar@indiatimes.com

(Received on: 17-02-12; Accepted on: 13-03-12)

ABSTRACT

Network security is very important in the internet and other form of electronic communications such as mobile communications, Pay-TV, e- commerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords etc, which touches on many aspects of our daily lives.

In this paper we proposed a new method of cryptography, in which we used Laplace transform for encrypting the plain text and corresponding inverse Laplace transform for decryption. Starting with basic theory of Laplace transforms in section 2, we obtained the main result in section 3. The generalization of the results is included in section 4.This paper is extension of the work of [4].

Key words: *Encryption, Decryption, Laplace Transforms, key.*

1. INTRODUCTION

Laplace transform has many applications in various fields such as Mechanics, Electrical circuit, Beam problems, Heat conduction, Wave equation, Transmission lines, Signals and Systems, Control systems, Communication Systems, Hydrodynamics, Solar systems,[5, 9]. In this paper we discuss its application to cryptography.

The fundamental objective of cryptography is to enable two people, to communicate over an insecure channel in such a way that an opponent cannot understand what is being said. Encryption is the process of obscuring information to make it unreadable without special knowledge. This is usually done for secrecy and typically for confidential communications. A cipher is an algorithm for performing encryption (and the reverse, decryption) a series of well-defined steps that can be followed as a procedure. The original information is known as plaintext, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it. Ciphers are usually parameterized by a piece of auxiliary information, called a key. The encrypting procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt, or more importantly, to decrypt, [1, 2, 3, 4, 6, 7, 8, 10, 11].

2. DEFINITIONS AND STANDARD RUSELTS

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

$$L\left\{f(t)\right\} = F(s) = \int_0^\infty e^{-st} f(t)\,dt \tag{2.1}$$

provided that the integral exists. Here the parameter s is a real or complex number. The corresponding inverse Laplace transform is $L^{-1}\{F(s)\} = f(t)$. Here $f(t)$ and $F(s)$ are called as pair of Laplace transforms, [5, 9].

2.2. Theorem: Laplace transform is a linear transform. That is, if
$L\{f_1(t)\} = F_1(s), L\{f_2(t)\} = F_2(s),$ then $L\{c_1 f_1(t) + c_2 f_2(t)\} = c_1 L\{f_1(t)\} + c_2\{f_2(t)\}$
where c_1 and c_2 are constants.

***Corresponding author: A.P. Hiwarekar*, *E-mail: anilhiwarekar@indiatimes.com**

The above result can easily be generalized to more than two functions, [5, 9].

2.3. LAPLACE TRANSFORMS OF ELEMENTARY FUNCTIONS:

Elementary functions include algebraic and transcendental functions.

1. $L\{t^n\} = \dfrac{n!}{s^{n+1}}, L^{-1}\{\dfrac{n!}{s^{n+1}}\} = t^n$
2. $L\{te^{kt}\} = \dfrac{1}{(s-k)^2},\ L^{-1}\{\dfrac{1}{(s-k)^2}\} = te^{kt}$, [5, 9].

3. PROPOSED WORK

3.1 ENCRYPTION

We consider standard expansion

$$e^{rt} = 1 + \frac{rt}{1!} + \frac{r^2t^2}{2!} + \frac{r^3t^3}{3!} + \cdots + \frac{r^nt^n}{n!} + \cdots + \cdots = \sum_{n=0}^{\infty} \frac{(rt)^n}{n!}, \tag{3.1}$$

where r is a constant, and

$$te^{rt} = t + \frac{rt^2}{1!} + \frac{r^2t^3}{2!} + \frac{r^3t^4}{3!} + \cdots + \frac{r^nt^{n+1}}{n!} + \cdots + \cdots = \sum_{n=0}^{\infty} \frac{r^nt^{n+1}}{n!}, \tag{3.2}$$

where r is a constant.

We allocated 0 to A and 1 to B then Z will be 25.

Let given message (plaintext) be 'PROFESSOR' it is equivalent to

15 17 14 5 4 18 18 14 17

Let $G_0 = 15$, $G_1 = 17$, $G_2 = 14$, $G_3 = 5$, $G_4 = 4$, $G_5 = 18$, $G_6 = 18$, $G_7 = 14$, $G_8 = 17$, $G_n = 0$ for n ≥ 9.

Let us consider

$$\begin{aligned} f(t) = Gte^{2t} &= t[G_0.1 + G_1\frac{2t}{1!} + G_2\frac{2^2t^2}{2!} + G_3\frac{2^3t^3}{3!} + G_4\frac{2^4t^4}{4!} + G_5\frac{2^5t^5}{5!} + G_6\frac{2^6t^6}{6!} + G_7\frac{2^7t^7}{7!} + G_8\frac{2^8t^8}{8!}] \\ &= 15t + 17\frac{2t^2}{1!} + 14\frac{2^2t^3}{2!} + 5\frac{2^3t^4}{3!} + 4\frac{2^4t^5}{4!} + 18\frac{2^5t^6}{5!} + 18\frac{2^6t^7}{6!} + 14\frac{2^7t^8}{7!} + 17\frac{2^8t^9}{8!} \\ &= \sum_{n=0}^{\infty} \frac{G_n 2^n t^{n+1}}{n!}. \end{aligned}$$

.

Taking Laplace transform on both sides we have

$$\begin{aligned} L\{f(t)\} &= L\{Gte^{2t}\} \\ &= L\{t[G_0.1 + G_1\frac{2t}{1!} + G_2\frac{2^2t^2}{2!} + G_3\frac{2^3t^3}{3!} + G_4\frac{2^4t^4}{4!} + G_5\frac{2^5t^5}{5!} + G_6\frac{2^6t^6}{6!} + G_7\frac{2^7t^7}{7!} + G_8\frac{2^8t^8}{8!}]\} \\ &= \frac{15}{s^2} + \frac{17(2)}{1!}\frac{2!}{s^3} + \frac{14(2^2)}{2!}\frac{3!}{s^4} + \frac{5(2^3)}{3!}\frac{4!}{s^5} + \frac{4(2^4)}{4!}\frac{5!}{s^6} + \frac{18(2^5)}{5!}\frac{6!}{s^7} + \frac{18(2^6)}{6!}\frac{7!}{s^8} + \frac{14(2^7)}{7!}\frac{8!}{s^9} + \frac{17(2^8)}{8!}\frac{9!}{s^1}. \\ &= \frac{15}{s^2} + \frac{68}{s^3} + \frac{168}{s^4} + \frac{160}{s^5} + \frac{320}{s^6} + \frac{3456}{s^7} + \frac{8064}{s^8} + \frac{14336}{s^9} + \frac{39168}{s^{10}} \end{aligned}$$

Now let q_i $for\ i = 0,1,2,3,\cdots$ be

$$15 = 26(0)+15, \quad 68 = 26(2)+16, \quad 168 = 26(6)+12,$$
$$160 = 26(6)+4, \quad 320 = 26(12)+8, \quad 3456 = 26(132)+24,$$
$$8064 = 26(310)+4 \bmod 26, \quad 14336 = 26(551)+10, \quad 39168 = 26(1506)+12.$$

That is

$$15 = 15 \bmod 26, \quad 68 = 16 \bmod 26, \quad 168 = 12 \bmod 26,$$
$$160 = 4 \bmod 26, \quad 320 = 8 \bmod 26, \quad 3456 = 24 \bmod 26,$$
$$8064 = 4 \bmod 26, \quad 14336 = 10 \bmod 26, \quad 39168 = 12 \bmod 26.$$

Let $G'_i = r_i = q_i - 26k_i$, $for\ i = 0,1,2,3,\cdots$ hence we get

$$G'_0 = 15, \quad G'_1 = 16, \quad G'_2 = 12, \quad G'_3 = 4, \quad G'_4 = 8, \quad G'_5 = 24,$$
$$G'_6 = 4, \quad G'_7 = 10, \quad G'_8 = 12, \quad G'_n = 0 \text{ for } n \ge 9,$$

with key k_i $for\ i = 0,1,2,3,\cdots$ as 0 2 6 6 12 132 310 551 1506.

Hence messages ‘PROFESSOR’ get converted to ‘PQMEIYEKM’.

3.2 DECRYPTION

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

15 16 12 4 8 24 4 10 12 .

Let

$$G'_0 = 15,\ G'_1 = 16,\ G'_2 = 12,\ G'_3 = 4,\ G'_4 = 8,\ G'_5 = 24,\ G'_6 = 4,\ G'_7 = 10,\ G'_8 = 12,\ G'_n = 0 \text{ for } n \ge 9.$$

Using given key k_i $for\ i = 0,1,2,3,\cdots$ as 0 2 6 6 12 132 310 551 1506, and assuming $q_i = 26k_i + G'_i$ $for\ i = 0,1,2,3,\cdots$.

Now we consider

$$G\frac{1}{(s-2)^2} = \frac{15}{s^2} + \frac{68}{s^3} + \frac{168}{s^4} + \frac{160}{s^5} + \frac{320}{s^6} + \frac{3456}{s^7} + \frac{8064}{s^8} + \frac{14336}{s^9} + \frac{39168}{s^{10}}.$$
$$= \sum_{n=0}^{\infty} \frac{q_i}{s^{n+2}},$$

Taking inverse transform we get

$$f(t) = Gte^{2t} = 15t + 17\frac{2t^2}{1!} + 14\frac{2^2t^3}{2!} + 5\frac{2^3t^4}{3!} + 4\frac{2^4t^5}{4!} + 18\frac{2^5t^6}{5!} + 18\frac{2^6t^7}{6!} + 14\frac{2^7t^8}{7!} + 17\frac{2^8t^9}{8!}.$$

Here we have $G_0 = 15$, $G_1 = 17$, $G_2 = 14$, $G_3 = 5$, $G_4 = 4$, $G_5 = 18$, $G_6 = 18$, $G_7 = 14$, $G_8 = 17$, $G_n = 0$ for $n \ge 9$.

Hence 15 17 14 5 4 18 18 14 17 is equivalent to ‘PROFESSOR’.

4. GENERALIZATION

For encryption of given message in terms of G_i we consider $f(t) = Gte^{rt}$, $r \in N$, where N is the set of natural numbers. Taking Laplace transform and we follow the procedure discussed in section 3, then we can convert the given message G_i to G'_i

where $G_i' = G_i r^i (i+1) \mod 26 = q_i \mod 26$ $where$ $q_i = G_i r^i (i+1)$ $i = 0,1,2,\cdots,$, with key $k_i = \frac{q_i - G'_i}{26}$ for $i = 0,1,2,3,\cdots.$

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

$$G\frac{1}{(s-k)^2} = \sum_{n=0}^{\infty}\frac{q_i}{s^{n+2}}$$

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

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

Remark: Results in [4] are now a special case of our results of section 4 with $r = 1.$

$$G\frac{1}{(s-k)^2} = \sum_{n=0}^{\infty}\frac{q_i}{s^{n+2}}$$

4.1. ILLASTRATIVE EXAMPLES

We have original message

1. ‘PROFESSOR’ gets converted to ‘PYOUIKWYZ’ with key as
   0 3 14 20 62 1009 3532 9420 38608, for $r = 3.$
2. ‘PROFESSOR’ gets converted to ‘PEEWYSEWR’ with key as
   0 9 79 263 1846 69813 570145 3547569 33923636, for $r = 7.$
3. ‘PROFESSOR’ gets converted to ‘POKEUUEMK’ for $r = 18.$

5. CONCLUDING REMARKS

In the proposed work a new cryptographic scheme is introduced using Laplace 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. The results in section 4 provide as many transformations as per the requirements which are the most useful factor for changing key.

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.

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] **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, July, 2011, 19-23.

[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**] Grewal B.S. –** Higher Engineering Mathematics, Khanna Pub. Delhi, 2005.

[6] **Lerma M. A. –** Modular Arithmetic, http//www.math.northwestern.edu/mlerma/proble m solving /results/ modular arith.pdf.

[7] **Petersen K.** – Notes on Number Theory and Cryptography, http://www.math.unc.edu/ Faculty petersen/ Coding/cr2.pdf.

[8] **Overbey J. - Traves W. and Wojdylo J.** – On the Key space of the Hill Cipher, Cryptologia, 29(1), January 2005, 59-72.

[9] **Ramana B.V.** – Higher Engineering Mathematics, Tata McGraw-Hills, 2007.

[10] **Saeednia- S.** – How to Make the Hill Cipher Secure, Cryptologia, 24(4), October 2000, 353-360.

[11] **Stallings W.** – Cryptography and network security, 4th edition, Prentice Hall, 2005.

****