International Journal of Mathematical Archive-2(12), 2011, Page: 2515-2519
Available online through www.ijma.info ISSN 2229 – 5046

A CRYPTOGRAPHIC SCHEME OF LAPLACE TRANSFORMS

G. Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar*

[1, 2, 3]Professor, Dept of Mathematics, GIT, GITAM University, INDIA

E-mail: nagalakshmi_g@gitam.edu, ravikumarbrk6@gitam.edu, acs@gitam.edu

(Received on: 18-11-11; Accepted on: 09-12-11)

ABSTRACT

Cryptography is the science of transmission and reception of secret messages. Recently electronic communication has become an essential part of every aspect of human life. Message encryption has become very essential to avoid the threat against possible attacks by hackers during transmission process of the message. Mathematical models playing a vital role in cryptanalysis. In the present paper a new cryptographic scheme is proposed using Laplace Transforms.

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

---

1. INTRODUCTION:

The fundamental objective of cryptography is to enable two people to communicate over an insecure channel in such a way that any opponent cannot understand what is being said. Communications security is gaining importance as a result of the use of electronic communications in more and more business activities. Cryptography is the only practical means to provide security services and is becoming a powerful tool in many applications for information security. 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. [1], [2]

A cipher is an algorithm for performing encryption and decryption. The original information is known as plain text and the encrypted form as cipher text. The cipher text message contains all the information of the plain text message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it. It should resemble random gibberish to those no intended to read 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 apt key the decryption is highly impossible.

1.1 LAPLACE TRANSFORMS:

Let f (t) is a function defined for all positive values of t. Then the Laplace transform of f (t), denoted by L {f (t)} or $\overline{f}$ (s) is defined by L {f (t)} = $\overline{f}$ (s) = $\int_0^\infty e^{-st} f(t)dt$ (1)

Provided that the integral exists. Here the parameter s is a real or complex number. The relation (1) can also be written as f (t) = $L^{-1}\{\overline{f}(s)\}$. In such a case, the function f (t) is said to be *inverse Laplace transform of* $\overline{f}$ *(s).* The symbol L which transforms f (t) into $\overline{f}$ (s) can be called the Laplace transform operator. The symbol L^{-1} which transforms $\overline{f}$ (s) to f (t) can be called the inverse Laplace transform operator. [7], [8]

1.2 LINEARITY PROPERTY:

If L {f (t)} = $\overline{f}$ (s) and L {g(t)} = $\overline{g}$ (s) then

L {c_1 f (t) + c_2 g (t)} = c_1 L {f (t)} + c_2 L {g(t)} = c_1 $\overline{f}$ (s) + c_2 $\overline{g}$ (s), where c_1 and c_2 are constants.

***Corresponding author:** A. Chandra Sekhar**, ***E-mail:** acs@gitam.edu*

The above result can easily be generalized to more than two functions.

Hence the Laplace transform of the sum of two or more functions of t is the sum of the Laplace transforms of the individual functions. Similarly inverse Laplace transforms also.

1.3 LAPLACE TRANSFORMS OF ELEMENTARY FUNCTIONS:

Elementary functions include Algebraic and transcendental functions**.** From the definition and by ordinary integration, we obtain **L** $\{t^n\} = \frac{n!}{s^{n+1}}$ where n is a positive integer [3],[4].

Similarly $L^{-1}\{\frac{1}{s^{n+1}}\} = \frac{t^n}{n!}$, $L^{-1}\{\frac{1}{(s-a)}\} = e^{at}$ and so on.

2. PROPOSED WORK:

We have $e^t = 1+\frac{t}{1!}+\frac{t^2}{2!}+\frac{t^3}{3!}+\frac{t^4}{4!}+\frac{t^5}{5!}+\frac{t^6}{6!}+\frac{t^7}{7!}+\frac{t^8}{8!}+----\infty$

2.1 Encryption:

Suppose sender wants to send the message "PROFESSOR". Consider

$$e^t = 1+\frac{t}{1!}+\frac{t^2}{2!}+\frac{t^3}{3!}+\frac{t^4}{4!}+\frac{t^5}{5!}+\frac{t^6}{6!}+\frac{t^7}{7!}+\frac{t^8}{8!}$$

$$te^t = t+\frac{t^2}{1!}+\frac{t^3}{2!}+\frac{t^4}{3!}+\frac{t^5}{4!}+\frac{t^6}{5!}+\frac{t^7}{6!}+\frac{t^8}{7!}+\frac{t^9}{8!}$$

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

Therefore now convert the message

"PROFESSOR" in the above pattern the converted form is 15 17 14 5 4 18 18 14 17. Writing these numbers as the co-efficient in "t e^t" we have

$$te^t = 15t+17\frac{t^2}{1!}+14\frac{t^3}{2!}+5\frac{t^4}{3!}+4\frac{t^5}{4!}+18\frac{t^6}{5!}+18\frac{t^7}{6!}+14\frac{t^8}{7!}+17\frac{t^9}{8!}$$

$$te^t = 15t+17t^2+7t^3+\frac{5}{6}t^4+\frac{t^5}{6}+\frac{3}{20}t^6+\frac{t^7}{40}+\frac{t^8}{360}+\frac{17}{40320}t^9$$

Taking Laplace Transforms on both side

$$\Rightarrow L\{te^t\} = L\{15t + 17t^2 + 7t^3 + \frac{5}{6}t^4 + \frac{1}{6}t^5 + \frac{3}{20}t^6 + \frac{1}{40}t^7 + \frac{1}{360}t^8 + \frac{17}{40320}t^9\}.$$

$$\Rightarrow \frac{1}{(s-1)^2} = 15\frac{1!}{s^2} + 17\frac{2!}{s^3} + 7\frac{3!}{s^4} + \frac{5}{6}\frac{4!}{s^5} + \frac{1}{6}\frac{5!}{s^6} + \frac{3}{20}\frac{6!}{s^7} + \frac{1}{40}\frac{7!}{s^8} + \frac{1}{360}\frac{8!}{s^9} + \frac{17}{40320}\frac{9!}{s^{10}}$$

$$\Rightarrow \quad \frac{1}{(s-1)^2} = \frac{15}{s^2} + \frac{34}{s^3} + \frac{42}{s^4} + \frac{20}{s^5} +$$
$$\frac{20}{s^6} + \frac{108}{s^7} + \frac{126}{s^8} + \frac{112}{s^9} + \frac{153}{s^{10}}$$

Adjusting the values 15 34 42 20 20 108 126 112 153 to mod 26. The resultant values are 15 8 16 20 20 4 22 8 23.

Sender send the values are 0 1 1 0 0 4 4 4 5 as private key

Let r = q - 26*key then 15 = 15 - 26 * 0; 8 = 34 - 26 * 1; 16 = 42 - 26 * 1; 20 = 20 - 26 * 0; 20 = 20 - 26 * 0; 4 = 108 - 26 * 4; and so on.

The resultant expansion is

$$\Rightarrow \quad \frac{1}{(s-1)^2} = \frac{15}{s^2} + \frac{8}{s^3} + \frac{16}{s^4} +$$
$$\frac{20}{s^5} + \frac{20}{s^6} + \frac{4}{s^7} + \frac{22}{s^8} + \frac{8}{s^9} + \frac{23}{s^{10}}.$$

The resultant values converted the message by using allotment

15 8 16 20 20 4 22 8 23

P I Q U U E W I X

Therefore the message converses “PROFESSOR” into “PIQUUEWIX”.

The sender publically sends the message and “t e^{t}”. Privately sends the key and The Laplace expansion. [5], [6]

2.2 Decryption:

The receiver receives the message “PIQUUEWIX”.

The equivalent values are

15 8 16 20 20 4 22 8 23
P I Q U U E W I X

and the private key values are

0 1 1 0 0 4 4 4 5.

Let q = 26*key + r then 15 = 26 * 0 + 15; 34 = 26 * 1 + 8; 42 = 26 * 1 + 16; 20 = 26 * 0 + 20; 20 = 26 * 0 + 20; 108 = 26 * 4 + 4 and so on.

we get 15 34 42 20 20 108 126 112 153

$$\Rightarrow \quad \frac{1}{(s-1)^2} = \frac{15}{s^2} + \frac{34}{s^3} + \frac{42}{s^4} + \frac{20}{s^5}$$
$$+ \frac{20}{s^6} + \frac{108}{s^7} + \frac{126}{s^8} + \frac{112}{s^9} + \frac{153}{s^{10}}.$$
$$\Rightarrow \quad \frac{1}{(s-1)^2} = \frac{15}{1!}\frac{1!}{s^2} + \frac{34}{2!}\frac{2!}{s^3} + \frac{42}{3!}\frac{3!}{s^4} + \frac{20}{4!}\frac{4!}{s^5} +$$
$$\frac{20}{5!}\frac{5!}{s^6} + \frac{108}{6!}\frac{6!}{s^7} + \frac{126}{7!}\frac{7!}{s^8} + \frac{112}{8!}\frac{8!}{s^9} + \frac{153}{9!}\frac{9!}{s^{10}}.$$

$$\Rightarrow \frac{1}{(s-1)^2} = 15\ \frac{1!}{s^2} + 17\ \frac{2!}{s^3} + 7\ \frac{3!}{s^4} + \frac{5}{6}\frac{4!}{s^5} + \frac{1}{6}\frac{5!}{s^6} + \frac{3}{20}\frac{6!}{s^7} + \frac{1}{40}\frac{7!}{s^8} + \frac{1}{360}\frac{8!}{s^9} + \frac{17}{40320}\frac{9!}{s^{10}}.$$

Taking inverse Laplace Transform on both sides

$$\Rightarrow L^{-1}\{\frac{1}{(s-1)^2}\} = L^{-1}\{15\ \frac{1!}{s^2} + 17\ \frac{2!}{s^3} + 7\ \frac{3!}{s^4} + \frac{5}{6}\frac{4!}{s^5} + \frac{1}{6}\frac{5!}{s^6} + \frac{3}{20}\frac{6!}{s^7} + \frac{1}{40}\frac{7!}{s^8} + \frac{1}{360}\frac{8!}{s^9} + \frac{17}{40320}\frac{9!}{s^{10}}\}.$$

$$\Rightarrow te^t = 15\frac{t^{2-1}}{(2-1)!} + 17\times 2!\frac{t^{3-1}}{(3-1)!} + 7\times 3!\frac{t^{4-1}}{(4-1)!} + \frac{5}{6}\times 4!\frac{t^{5-1}}{(5-1)!} + \frac{5!}{6}\frac{t^{6-1}}{(6-1)!} + \frac{3}{20}\times 6!\frac{t^{7-1}}{(7-1)!} + \frac{7!}{40}\frac{t^{8-1}}{(8-1)!} + \frac{8!}{360}\frac{t^{9-1}}{(9-1)!} + \frac{17}{40320}\times 9!\frac{t^{10-1}}{(10-1)!}.$$

$$\Rightarrow te^t = 15t + 17\times 2!\frac{t^2}{2!} + 7\times 3!\frac{t^3}{3!} + \frac{5}{6}\times 4!\frac{t^4}{4!} + \frac{5!}{6}\frac{t^5}{5!} + \frac{3}{20}\times 6!\frac{t^6}{6!} + \frac{7!}{40}\frac{t^7}{7!} + \frac{8!}{360}\frac{t^8}{8!} + \frac{17}{40320}\times 9!\frac{t^9}{9!}.$$

$$\Rightarrow te^t = 15\ t + 17\ t^2 + 7\ t^3 + \frac{5}{6}t^4 + \frac{1}{6}t^5 + \frac{3}{20}t^6 + \frac{1}{40}t^7 + \frac{1}{360}t^8 + \frac{17}{40320}t^9.$$

$$\Rightarrow te^t = 15t + 17\times 1!\frac{t^2}{1!} + 7\times 2!\frac{t^3}{2!} + \frac{5}{6}\times 3!\frac{t^4}{3!} + \frac{4!}{6}\frac{t^5}{4!} + \frac{3}{20}\times 5!\frac{t^6}{5!} + \frac{6!}{40}\frac{t^7}{6!} + \frac{7!}{360}\frac{t^8}{7!} + \frac{17}{40320}\times 8!\frac{t^9}{8!}.$$

$$\Rightarrow te^t = 15\ t + 17\ t^2 + 14\ \frac{t^3}{2!} + 5\ \frac{t^4}{3!} + 4\ \frac{t^5}{4!} + 18\ \frac{t^6}{5!} + 18\ \frac{t^7}{6!} + 14\ \frac{t^8}{7!} + 17\ \frac{t^9}{8!}.$$

$$\Rightarrow e^t = 15\ + 17\ t^1 + 14\ \frac{t^2}{2!} + 5\ \frac{t^3}{3!} + 4\ \frac{t^4}{4!} + 18\ \frac{t^5}{5!} + 18\ \frac{t^6}{6!} + 14\ \frac{t^7}{7!} + 17\ \frac{t^8}{8!}.$$

In the above expansion the co-efficient are 15 17 14 5 4 18 18 14 17

We know that

$$e^t = 1+\frac{t}{1!}+\frac{t^2}{2!}+\frac{t^3}{3!}+\frac{t^4}{4!}+\frac{t^5}{5!}+\frac{t^6}{6!}+\frac{t^7}{7!}+\frac{t^8}{8!}+----\infty$$

Then we get the message is

15 17 14 5 4 18 18 14 17

P R O F E S S 0 R as required.

3. CONCLUSIONS:

In the proposed work a new cryptographic scheme is introduced using Laplace Transforms and the private key is the number of multiples of mod n. Therefore it is very difficult for an eyedropper to trace the private key either by the Brute farce attack or by any other attack.

4. REFERNCES:

[1] A.P. Stakhov, "The golden matrices and a new kind of cryptography", Chaos, Soltions and Fractals 32((2007) pp1138–1146

[2] A.P. Stakhov. "The golden section in the measurement theory". Compute Math Appl; 17(1989):pp613–638.

[3] W. Diffie and M. E. Hellman. "New directions in cryptography. IEEE Transactions on Information Theory". 22, 633-654, 1976.

[4] A text book of "Laplace Transforms" by Murray R. Spiegel. Schaum's ouTlines.

[5] Chen-Hun-Chen, YenJui-Cheng and Guo Juin-In, "Design a New Cryptography system", Lecture Notes in Computer Science 2002, Vol. 2532/2002, 211-219.

[6] Hun-Chen Chen, Jui Cheng Yen, "A new Cryptography systems and its VISI Realization", Journal of Systems Architecture, Vol.49, Issues 7-9,

[7] Martine Hell and Thomas Johnson, "Breaking the Stream Cipher F-FCSR-H and F-FCSR-16 in Real Time", Journal of Cryptology, October 2009.

[8] "Data Encryption Technique using random number generator, published in the IEEE International Conference on Granular Technology Grc07, Nov 2-4 2007, Silicon Valley, USA, pp576-579.

****

