Southeast Europe Journal of Soft Computing ISSN 2233 – 1859
Available online: http://scjournal.ius.edu.ba

Vol 12, No. 2, September 2023, pp. 10-14

A cryptographic technique applying Laplace Transform and Exponetial Function

[1*]Mohib Rasool and [2]Kala Raja Mohan

[1]*Department of Computer Science Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,*

#400 feet outer Ring Road, Avadi, Chennai-600062, INDIA

[2]*Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,*

#400 feet outer Ring Road, Avadi, Chennai-600062, INDIA

**Corresponding Author*: *mohibrasool004@gmail.com*

Article Info

Article history:

Article received on 09 10 2023

Received in revised form 29 10 2023

Keywords:

Cryptography, hyperbolic sine function, Laplace Transform

ABSTRACT: Secured Information transformation from one person to another is very much essential in this world of internet. In electronic communications such as system security, smart card, mobile communications etc, the data are stored in the various applications used in them. While using all the applications, we give permission to access all the information. Cryptography is based on transformation of multiple rounds of transformation of messages in the form of plain text as input into encrypted text message. Through suitable mathematical technique, secrecy of the information is maintained. This paper proposes a Laplace and its inverse transform technique with a suitable function for encryption and decryption of a message.

1. INTRODUCTION

In Universe, computer networks, internet and mobile communications are more important and unavoidable part of our society, so that information security is obviously required to protect from hackers. One of the widely used approaches for information security is Cryptography. The mathematic of encryption, plays a major role in many fields. The main goal of cryptography is to ensure the secret communication between two individuals. Encryption is the process of obscuring information to make it unreadable without special knowledge.

Laplace transform find its application in many fields. In Cryptography also, it plays a significant role. A new cryptographic technique applying Laplace transform is carried out. For this purpose, the exponential expansion function is used.

A. P. Hiwarekar in 2014 proposed two cryptographic technique applying Laplace Transform and Hyperbolic functions [1,3]. M. Tuncay Gencoglu in 2017 introduced a crytographic process involving Laplace Transform with Hyperbolic functions [2]. Dr. K. Hemant K. Undegaonkar introduced a secured communication method involving Laplace Transform

[4]. S. Sujatha in 2013 made use of the application of Laplace Transform in the field of cryptography [5]. C. H. Jayanthi and V. Srinivas in 2019 framed a new mathematical modelling involving Laplace Transform [6]. G. Nagalakshmi et al in 2020 involved Laplace Transform Laplace Transform using Asymmetric key for secured communication [7]. S. Dhingra et al proposed a network security method involving Laplace Transform [8]. M. Saha in 2017 utilized Laplace Mellin Transform in forming a cryptographic method for secured information sharing [9]. A. K. H. Sedeeg et al in 2016 formulated a new cryptographic algorithm applying Aboodh Transform [10].

Kala Raja Mohan et al in 2022 applied Bilinear Transform with Probability in identifying a secured information sharing algorithm [11]. A. Meenakshi et al applied graph network in designing a crypographic algorithm [12]. Kala Raja Mohan et al in 2022 made use of Laplace transform and hyperbolic tangent function in cryptography [13]. This paper aims at developing a cryptographic algorithm using fuzzy logic.

In this paper, section 2 describes the standard definitions applied in this crypto analysis. Section 3 presents the algorithm for encryption. Section 4 demonstrates the algorithm explained in section 3 with an example. Section 5 depicts the algorithm applied for decryption. With the help of the cipher text obtained in Section 4, decryption process is explained in section 6. Section 7 is about the conclusion followed by references.

2. STANDARD DEFINITIONS

The following standard definitions are applied in the cryptographic analysis in this paper.

- **Cipher Text**

The transformed form of plain text, which can be read only using the key specified by the sender is called the cipher text.

- **Plain Text**

Plain text is the data which can be directly read by any person. It is the information which has to be shared secretly to the receiver..

- **Cipher**

Cipher refers to the algorithm through which the plain text is transformed to cipher text.

- **Encryption**

Encryption is the process in which the given information is converted into secret message. This hides the original information reaching unauthorized persons, using the secret key.

- **Decryption**

Decryption is the reverse process of Encryption. This is the process in which the encrypted text gets converted into original text with the usage of the secret key.

- **Laplace Transform**

Laplace transform of a function $f(t)$ is given by $F(s) = \int_0^\infty f(t)e^{-st}dt$ where t is a real number. The Laplace transform of t^n given by $L(t^n) = \frac{n!}{s^{n+1}}$ is used for the Encryption process in this paper.

- **Inverse Laplace Transform**

The function which has given the Laplace transform is found using the inverse Laplace transform given by $f(t) = L^{-1}\{F(s)\}$

The inverse Laplace transform of $\frac{1}{s^n}$ given by $L^{-1}\left\{\frac{1}{s^n}\right\} = \frac{t^{n-1}}{(n-1)!}$Is used for the Decryption process in this paper.

- **Hyperbolic functions**

Hyperbolic functions are similar to ordinary trigonometric functions, which are defined using hyperbola. The hyperbolic expansion of sine function is applied in this Cryptographic analysis.

- **Modulus functions**

The absolute value of a number is given by modulus function.

- **Modulo Operator**

The modulo operator gives the remainder value when one number is divided by another number

3. ALGORITHM FOR ENCRYPTION

The step-by-step procedure to be carried out in encryption are as follows.

Step 1: Assuming 0 to A, 1 to B and so on., the numerical equivalent of the given plain text is generated. These numerical values for each alphabet of the plain text are assigned to variable G with suffix 0,1, 2,... based on the count of the alphabets.

Step 2: Using the expansion of exponential function, the function $\boldsymbol{f(t)}$ is formulated using the relation $\boldsymbol{f(t) = G\, t^2\, e^{ax}}$

Step 3: Laplace Transform is applied to the function $\boldsymbol{f(t)}$.

Step4: The modulus value for each of the coefficient of the Laplace transform of $\boldsymbol{f(t)}$ is assigned to the variable E with suffix 0, 1, 2, ...

Step 5: To the above obtained values, the cipher text is obtained.

4. ENCRYPTION PROCESS

The encryption process carried out is explained in this section with an example. The encryption procedure is applied to the plain text MOTHER and its cipher text is obtained.

$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots x$

where, $k_0 = 0;\ k_1 = 1;\ k_2 = 2;\ k_3 = 7;\ k_4 = 9;$ ...

$$e^{ax} = 1 + \frac{ax}{1!} + \frac{(ax)^2}{2!} + \frac{(ax)^3}{3!} + \cdots$$

M	O	T	H	E	R
12	14	19	7	4	17

Assume $G_0 = 12;\ G_1 = 14;\ G_2 = 19;\ G_3 = 7;\ G_4 = 4;\ G_5 = 17;\ G_n = 0\ for\ n \geq 6$

Taking $a = 2;$

$$e^{2x} = 1 + \frac{2x}{1!} + \frac{4\,(x^2)}{2!} + \frac{8\ (x^3)}{3!} + \cdots$$

For the purpose of Encryption assume the function

$f(t) = G\ t^2 e^{2t}$

$$= (12)\,(t^2) + (14)\frac{(2)\,(t^3)}{1!} + (19)\frac{(4)\,(t^4)}{2!} + (7)\frac{(8)\ (t^5)}{3!} + (4)\frac{(16)\ (t^6)}{4!} + \{17)\frac{(32)\ (t^7)}{5!}$$

Applying Laplace Transform

$$L\{f(t)\} = L\{G\ t^2\ sinh\ 2t\} = \frac{(24)}{(s^3)} + \frac{(168)}{(s^4)} + \frac{(912)}{(s^5)} + \frac{(1120)}{(s^6)} + \frac{(1920)}{(s^7)} + \frac{(22848)}{(s^8)}$$

Adjusting the resultant values using modulus function

24 168 912 1120 1920 22848

to mod 26, it becomes

$$24 = 24\ mod\ 2$$

$$168 = 12\ mod\ 26$$

$$912 = 2\ mod\ 26$$

$$1120 = 2\ mod\ 26$$

$$1920 = 22\ mod\ 26$$

$$22848 = 20\ mod\ 26$$

Sender receives the key vales as shown below:

0 6 35 43 73 878

Assuming $E_0 = 24;\ E_1 = 12;\ E_2 = 2;\ E_3 = 2;\ E_4 = 22;\ E_5 = 20;\ E_n = 0\ for\ n \geq 6$

24	12	2	2	22	20
Y	M	C	C	W	U

5. ALGORITHM FOR DECRYPTION

Decryption is the reverse process of encryption. In this stage the cipher text gets converted to plain text. The process of decryption has the following steps to be performed.

Step 1: The values of $\boldsymbol{E_n}$ and the corresponding key $\boldsymbol{K_n}$ are obtained.

Step 2: $\boldsymbol{q_n = E_n + 26\ K_n}$ and $\boldsymbol{G(s)} = \sum \quad \frac{q_n}{s^{n+3}}$

Step 3: Apply inverse Laplace Transform to G(s) and obtain $\boldsymbol{g(t)}$.

Step 4: $\boldsymbol{g(t)}$ can be written as $\boldsymbol{G\ t^2}\ e^{2t}$

Step 5: From $g(t)$, the plain text is obtained assuming 0 to A, 1 to B and so on.

6. DECRYPTION PROCESS

During the decryption process, the received cipher text is processed in the reverse direction of encryption process. For this purpose, inverse Laplace transform is applied.

For the above example the cipher text received is 'YMCCWU'.

This is equivalent to

24 12 2 2 22 20

Assume $E_0 = 24;\ E_1 = 12;\ E_2 = 2;\ E_3 = 2;\ E_4 = 22;\ E_5 = 20;$

Using the key

0 6 35 43 73 878

and taking $q_n = E_n + 26\ K_n\ ; n = 0,1,2,3,4,5$

Consider $G(s) = \sum_{n=0}^{5} \quad \frac{q_n}{s^{n+3}}$

$$G(s) = \frac{(24)}{(s^3)} + \frac{(168)}{(s^4)} + \frac{(912)}{(s^5)} + \frac{(1120)}{(s^6)} + \frac{(1920)}{(s^7)} + \frac{(22848)}{(s^8)}$$

Applying inverse Laplace transform and rearranging

$$L^{-1}\{G(s)\} = (12)\ (t^2) + (14)\frac{(2)\ (t^3)}{1!} + (19)\frac{(4)\ (t^4)}{2!} + (7)\frac{(8)\ \ (t^5)}{3!} + (4)\frac{(16)\ \ (t^6)}{4!} + \{17)\frac{(32)\ \ (t^7)}{5!}$$

which can be written as $g(t) = G\ t^2\ e^{2t}$

From the above expression, the decryption values are $G_0 = 12;\ G_1 = 14;\ G_2 = 19;\ G_3 = 7;\ G_4 = 4;\ G_5 = 17;$

which is equivalent to

12	14	19	7	4	17
M	O	T	H	E	R

7. CONCLUSION

A new cryptographic algorithm applying Laplace and inverse Laplace transform to the expansion of exponential function has been proposed. The plain text MOTHER has been converted to cipher text using the proposed Encryption algorithm. Also its reverse process using Decryption algorithm has been furnished to get the plain text.

REFERENCES

[1] A. P. Hiwarekar, "New mathematical modeling for cryptography," *Journal of Information Assurance and Security*, **9**, 027-033 (2014).

[2] M. Tuncay Gencoglu, "Cryptanalaysis of a New Method of Cryptography using Laplace Transform Hyperbolic Functions." *Communications in Mathematics and Applications*, **8**, 183-189 (2017).

[3] A. P. Hiwarekar, "A new method of Cryptography using Laplace transform of Hyperbolic functions," *International Journal of Mathematical Archive*, **4**, 208-213 (2013).

[4] Dr. K. Hemant K. Undegaonkar, "Security in Communication By Using Laplace Transform and Cryptography," *International Journal of Scientific & Technology Research*, **8**, 3207-3209 (2019).

[5] S. Sujatha, "Application of Laplace Transforms in Cryptography," *International Journal of MathematicalArchive*, **4**, 67-71 (2013).

[6] C. H. Jayanthi and V. Srinivas, "Mathematical Modelling for Cryptography using Laplace Transform," *International Journal of Mathematics Trends and Technology*, **65**, 10-15 (2019).

[7] G. Nagalakshmi, A. Chandra Sekhar and D. Ravi Sankar, "Asymmetric key Cryptography using Laplace Transform," *International Journal of Innovative Technology and Exploring Engineering*, **9**, 3083-3087 (2020).

[8] S. Dhingra, A. A. Savalgi and S. Jain, “Laplace Transformation based Cryptographic Technique in NetworkSecurity,” *International Journal of Computer Applications*, **136**, 6-10 (2016).

[9] M. Saha, “Application of Laplace – Mellin Transform for Cryptography,” *Raj Journal of Technology Research & Innovation*, **5**, 12-17 (2017).

[10] A. K. H. Sedeeg, M. M. Abdelrahim Mahgoub, and M. A. Saif Saeed, “An Application of the New Integral “Aboodh Transform” in Cryptography,” *Pure and Applied Mathematics Journal*, **5**, 151-154 (2016).

[11] Kala Raja Mohan, Suresh Rasappan, Regan Murugesan, Sathish Kumar Kumaravel and Ahamed A. Elngar,“Secret Information Sharing Using Probability and Bilinear Transformation”, *Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science*, 115-122 (2022).

[12] A. Meenakshi, J. Senbagamalar, and A. Neel Armstrong, “Encryption on Graph Networks”**,** *Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science*, 123-130 (2022).

[13] Kala Raja Mohan, Suresh Rasappan and Sathish Kumar Kumaravel, “Secret Information sharing Using Laplace Transform and Hyperbolic Tangent Function”, *AIP Conference Proceedings 2516, 12003*, 1-6, (2022).