ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha*, Vol. 53(1) (2023), 106-109**
(Dedicated to Professor G. C. Sharma on His 85^{th} Birth Anniversary Celebrations)

CRYPTANALYSIS USING LAPLACE TRANSFORM OF ERROR FUNCTION

Rinku Verma, Pranjali Kekre* and Keerti Acharya
Department of Mathematics, Medi-Caps University, Pigdamber, Rau, Madhya Pradesh, India-453331
Email: rinku.verma@medicaps.ac.in, pranjali.kekre@medicaps.ac.in, keerti.sharma@medicaps.ac.in.
(Received: August 05*, 2022; In format: August* 13*, 2022; Revised: January* 30*, 2023; Accepted: February* 04*, 2023)*

DOI: https://doi.org/10.58250/jnanabha.2023.53113

Abstract

This paper presents a new cryptographic scheme for encryption and decryption by introducing the Laplace transform of error function. Here we have used the concept of congruence relation and modular arithmetic to find symmetric key, cipher text and Decryption process. The implementation has been done using Matlab.

2020 Mathematical Sciences Classification: 11A07, 44A10, 94A60, 11T71
Keywords and Phrases: Laplace transform, network security, error function, cipher text, symmetric key, congruence relation.

1 Introduction

Cryptography is a scientific technique related to aspects of information security such as data integrity, entity authentication and data origin authentication. Cryptography is a set of techniques to provide information security. It helps to store sensitive information, transmit it across insecure networks like internet so that it can't be read by anyone except the intended receiver.

Analysis of cryptographic security leads to using theoretical computer science especially complexity theory. The actual implementation of crypto systems and the hard work of carrying out security analysis for specific cryptosystems fall into engineering and practical computer science and computing. The persons or systems performing cryptanalysis in order to break a crypto system are called attackers. The process of such type of attacking is called hacking. Some cryptographic algorithms are very trivial to understand, replicate and therefore easily cracked. To secure the data from hackers it needs to be encrypted with high level of security.

Encryption and Decryption are carried forward using mathematical algorithms in cryptography. Initially Stanoyevitch [14] introduced cryptography with mathematical foundations and computer implementations. Overbey, Traves and Wojdylo [9] used technique of Hill cipher keyspace consist of all matrices that are invertible. Use of matrices for encryption and decryption were found by Dhanorkar and Hiwarekar[1]. After that [3,4, 5,8] used Laplace transform techniques for the cryptographic purpose by combining infinite series of various functions . Dhingra, Savalgi and Jain [2] presented new scheme for the cryptography by combining infinite series and Laplace transform using ASCII code. Genoglu [16] used a new method of cryptography using Lapalce transform of Hyperbolic function. Some interesting results are found in the literature [7, 10−13] regarding modular arithmetic and cryptography.

In this paper, the process of encryption is expanded using series of error function and taking its Laplace transform. On the basis of literature survey we found while using the cryptography on the basis of Laplace transform only functions with positive terms were considered so far, but in error function we have an alternating series, so we used the concept of congruence relation to change the sign of transformed series terms coefficients , and use modular arithmetic to find symmetric key , cipher text and Decryption process.

2 Some Basic Terminologies

2.1 Plain text

It signifies a message that can be understood by the sender, the recipient and also by anyone else who gets access to that message.

2.2 Cipher text

When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

2.3 Encryption and Decryption

Encryption transforms a plain text message into cipher text, whereas decryption transforms a cipher text message back into plain text.

2.4 Symmetric and Asymmetric Key

Cryptography algorithms classified mainly into two major types: Symmetric-key cryptography and public key (Asymmetric) cryptography [15]. In Symmetric-key cryptography, each sender and receiver shared the same key used to encrypt and decrypt data with disadvantage of key management required to keep the key secure. The Data Encryption Standard *(DES)* and the Advanced Encryption Standard *(AES)* are examples of Symmetrickey cryptography methods. In public-key cryptography, each sender and receiver use two different keys to encrypt and decrypt data - public key and private key-, the public key can be freely distributed, while its paired private key must remain secret. In public-key cryptography, we overcome the key management distribution issue of Symmetric-key cryptography, but at the expense of performance speed

2.5 Laplace transform

Laplace transform is useful out of many transformations that are used for security purposed and as per the requirement which is a useful factor for changing key where algorithm plays an important role. That's why it will be difficult for a hacker to trace the key by any mode. For any function $f(t), t \geq 0$ Laplace transform $L\{f(t)\}$ is defined as

$$L\{f(t)\} = \int_0^\infty e^{-st} f(t)dt = f(s),$$

where t is known as time domain parameter and S (may be real or complex) is known as frequency domain parameter.

2.6 Error Function

$$erf(\sqrt{t})\} = \frac{2}{\sqrt{\pi}} \int_0^{\sqrt{t}} e^{-u^2} du = \frac{2}{\sqrt{\pi}} \sum_{i=0}^{\infty} (-1)^i \frac{t^{(2i+1)/2}}{i!(2i+1)}.$$

3 Encryption Algorithm

The proposed algorithm uses the Laplace transform of error function to generate the cipher text and a sender key as symmetric encryption. In the beginning this secret key between sender and receiver is determined and shared on the basis of quotient reminder theorem and congruence relation.

Step 1: Sender and receiver agree on secret key.

Step 2: Select the message to be sent and convert each plain text alphabet into as a number in an increasing sequence as $A = 0, B = 1, C = 2, \ldots, Z = 25$.

Let the plain text is "*SUBJECT*" and it is equivalent to 1820194219.

Let $C_0 = 18, \mathrm{C}_1 = 20, \mathrm{C}_2 = 1, \mathrm{C}_3 = 9, \mathrm{C}_4 = 4, \mathrm{C}_5 = 2, \mathrm{C}_6 = 19$.

Step 3: Now writing these numbers as coefficients of $\mathrm{erf}(\sqrt{t})$, neglecting higher coefficients ($i \geq 7$) and considering $f(t) = C\,\mathrm{erf}(\sqrt{t})$,

we get

$$\begin{aligned} f(t) &= \frac{2}{\sqrt{\pi}} \left[C_0 t^{1/2} - \frac{C_1 t^{3/2}}{3} + \frac{C_2 t^{5/2}}{2!5} - \frac{C_3 t^{7/2}}{3!7} + \frac{C_4 t^{9/2}}{4!9} - \frac{C_5 t^{11/2}}{5!11} + \frac{C_6 t^{13/2}}{6!13} \right] \\ &= \frac{2}{\sqrt{\pi}} \sum_{i=0}^{\infty} (-1)^i \frac{t^{(2i+1)/2}}{i!(2i+1)} C_i. \end{aligned} \tag{3.1}$$

Step 4: Now taking Laplace transform of (3.1) , we get

$$L\{f(t)\} = \frac{2}{\sqrt{\pi}} L \left\{ C_0 t^{1/2} - \frac{C_1 t^{3/2}}{3} + \frac{C_2 t^{5/2}}{2!5} - \frac{C_3 t^{7/2}}{3!7} + \frac{C_4 t^{9/2}}{4!9} - \frac{C_5 t^{11/2}}{5!11} + \frac{C_6 t^{13/2}}{6!13} \right\}.$$

Using $L\{t^n\} = \frac{\Gamma(n+1)}{s^{n+1}}, (n+1) > 0$,

$$L\{f(t)\} = \frac{C_0}{s^{3/2}} - \frac{C_1}{2s^{5/2}} + \frac{3C_2}{2^3 s^{7/2}} - \frac{5C_3}{2^4 s^{9/2}} + \frac{105C_4}{2^6 s^{11/2}} - \frac{63C_5}{2^8 s^{13/2}} + \frac{231C_6}{2^{10} s^{15/2}}.$$

Alternating terms of the series are converted using congruence relation to integer modulo 26 .

$$L\{f(t)\} = \frac{C_0}{s^{3/2}} + \frac{25C_1}{2s^{5/2}} + \frac{3C_2}{2^3 s^{7/2}} + \frac{21C_3}{2^4 s^{9/2}} + \frac{105C_4}{2^6 s^{11/2}} + \frac{15C_5}{2^8 s^{13/2}} + \frac{231C_6}{2^{10} s^{15/2}}. \tag{3.2}$$

Substituting the values of $C_i i = 0, 1, 2, \ldots, 6$ and simplifying, we get

$$2^{10} L\{f(t)\} = \frac{18432}{s^{3/2}} + \frac{256000}{s^{5/2}} + \frac{384}{s^{7/2}} + \frac{12096}{s^{9/2}} + \frac{6720}{s^{11/2}} + \frac{120}{s^{13/2}} + \frac{4389}{s^{15/2}}.$$

Step 5: Now we calculate r_i using $r_i = M_i \bmod (26)$ and q_i as quotient

i	M_i	r_i	q_i
0	18432	24	708
1	256000	4	9846
2	384	20	14
3	12096	6	465
4	6720	12	258
5	120	16	4
6	4389	21	168

Hence the message "*SUBJECT*" is encrypted to "*YEUGMQV*" as cipher text and the symmetric secret key as 708 9846 14 465 258 4 168, delivered to receiver.

4 Decryption Algorithm

Steps involved in Decryption are as follows:

Step 1. Consider the cipher text and key received from the sender. In the above example cipher text is "*YEUGMQV*" and the secret key 708 9846 14 465 258 4 168.

Step 2 . Convert the given cipher text to a corresponding finite sequence of numbers, 24 4 20 6 12 16 21, comparing with (3.2) using modular arithmetic equivalent in mod 26, we get

$$C_0 \cdot 2^{10} = 26.K_0 + 24 \Rightarrow C_0 = \frac{26.K_0 + 24}{2^{10}} \Rightarrow \begin{cases} K_0 = 196 & C_{0,1} = 5 \\ K_0 = 708 & C_{0,2} = 18 \end{cases}$$

$$C_1 \cdot 2^9 \cdot 25 = 26.K_1 + 4 \Rightarrow C_1 = \frac{26.K_1 + 4}{2^9.25} \Rightarrow \begin{cases} K_1 = 3446 & C_{1,1} = 7 \\ K_1 = 9846 & C_{1,2} = 20 \end{cases}$$

$$C_2 \cdot 2^7 \cdot 3 = 26.K_2 + 20 \Rightarrow C_2 = \frac{26.K_2 + 20}{2^7 \cdot 3} \Rightarrow \begin{cases} K_2 = 14 & C_{2,1} = 1 \\ K_2 = 206 & C_{2,2} = 14 \end{cases}$$

$$C_3.2^6.21 = 26.K_3 + 6 \Rightarrow C_3 = \frac{26.K_3 + 6}{2^6.21} \Rightarrow \begin{cases} K_3 = 465 & C_{3,1} = 9 \\ K_3 = 1137 & C_{3,2} = 22 \end{cases}$$

$$C_4 \cdot 2^4.105 = 26.K_4 + 12 \Rightarrow C_4 = \frac{26.K_4 + 12}{2^4.105} \Rightarrow \begin{cases} K_4 = 258 & C_{4,1} = 4 \\ K_4 = 1098 & C_{4,2} = 17 \end{cases}$$

$$C_5 \cdot 2^2 \cdot 15 = 26.K_5 + 16 \Rightarrow C_5 = \frac{26.K_5 + 16}{2^2.15} \Rightarrow \begin{cases} K_5 = 4 & C_{5,1} = 2 \\ K_5 = 34 & C_{5,2} = 15 \end{cases}$$

$=$

Step 3. Now using the secret key 708 9846 14 465 258 4 168 we get required C_i's as 18,20 , $1, 9, 4, 2, 19$, now convert the numbers of above finite sequence to alphabets the original plain text is obtained as "*SUBJECT*".

5 Conclusion

The proposed algorithm give us an encrypted cipher text and after decryption we are getting a original plain text, thus the proposed method is valid and helpful in the case when an alternative series such as error function is used in cryptography. On the basis of modular arithmetic we get proper results instead of using sequential numbers as coefficients we can use ASCII code, with the same function for getting more secured chipper text and key.

In the proposed work we expand an innovative cryptographic scheme using Laplace transforms of error function and modular arithmetic functions.

Acknowledgement. We are thankful to Editors and Reviewers for their valuable suggestions to improve the article.

References

[1] G. A. Dhanorkar and A. Hiwarekar, A generalized Hill cipher using matrix transformation, *International J. of Math. Sci. and Engg. Appls.,* **5**(4) (July 2011), 19-23.

[2] S. Dhingra, A. Savalgi and S. Jain, Laplace Transformation based Cryptographic Technique in Network Security, *International Journal of Computer Applications,* **136**(7) (2016), 0975-8887.

[3] A. Hiwarekar, Application of Laplace Transform For Cryptographic Scheme, *Proceedings of the World Congress on Engineering WCE* 2013, London, U.K., **1** (July 2013), 1 - 7.

[4] A. Hiwarekar, A new method of cryptography using Laplace transform, *International Journal of Mathematical Archive,* **3**(3) (2012), 1193-1197.

[5] A. Hiwarekar, A new method of cryptography using Laplace transform of hyperbolic functions, *International Journal of Mathematical Archive,* **4**(2) (2013), 208-213.
[6] K. Kumar, L. Rathour, B. M. K. Sharma and V. N. Mishra, Fixed point approximation for suzuki generalized non expansive mapping using $B(\delta, \mu)$ condition, *Applied Mathematics,* **13**(2) (2022), 215-227.
[7] L. N. Mishra, V. Dewangan, V. N. Mishra and S. Karateke, Best proximity points of admissible almost generalized weakly contractive mappings with rational expressions on b-metric spaces, *J. Math. Computer Sci.,* **22**(2) (2021), 97-109. doi: 10.22436 / j m c s .022 .02 .01.
[8] G. N. Lakshmi, B. R. Kumar and A. C. Sekhar, A cryptographic scheme of Laplace transforms, *International Journal of Mathematical Archive,* **2** (2011), 2515-2519.
[9] J. Overbey , W .Traves and J Wojdylo, On the Keyspace of the Hill Cipher, *Cryptologia,* **29**(2005), 59-72.
[10] K. Paul, P. Goswami and M. M. Singh, Algebraic braid group public key cryptography, *Jñānābha*, **52**(2) (2022), 218-223.
[11] A. G. Sanatee, L. Rathour, V. N. Mishra and V. Dewangan, Some fixed point theorems in regular modular metric spaces and application to Caratheodory's type anti-periodic boundary value problem, *The Journal of Analysis,* (2022), DOI: https://doi.org/10.1007/s41478-022-00469https://doi.org/10.1007/s41478-022-00469
[12] P. Shahi, L. Rathour and V. N. Mishra, Expansive Fixed Point Theorems for tri-simulation functions, *The Journal of Engineering and Exact Sciences -JCEC*, **8**(3)(2022), 14303-01e. DOI: https://doi.org/10.18540/jcecvl8iss3pp14303-01ehttps://doi.org/10.18540/jcecvl8iss3pp14303-01e
[13] N. Sharma, L. N. Mishra, V. N. Mishra and S. Pandey, Solution of Delay Differential equation via $N^\mathbf{v}1$ iteration algorithm, *European J. Pure Appl. Math.,* **13**(5) (2020), 1110-1130. DOI: https://doi.org/10.29020/nybg.ejpam.v13i5.3756https://doi.org/10.29020/nybg.ejpam.v13i5.3756.
[14] A. Stanoyevitch, *Introduction to cryptography with mathematical foundations and computer implementations,* CRC Press, 2002.
[15] W.Stallings, *Cryptography and network security,* 4th edition, Prentice Hall, 2005.
[16] M. Tuncay Genoglu,-Cryptanalysis of A New Method of Cryptography using Laplace Transform Hyperbolic Functions, *Communications in Mathematics and Applications,* **8**(2) (2017), 183-189.