Mathematical Modelling for Cryptography using Laplace Transform

[1]CH. Jayanthi, [2]V.Srinivas
[1]Department of Mathematics, Vignana Bharathi Institute of Technology, Aushapur(V), Ghatkesar(M), Medchal Dist, Telangana, Pin-501301, India.
[2]Department of Mathematics, University College of Science, Saifabad, Osmania University.

Abstract

Information security is very significant in internet and other form of electronic communications such as system security, security of smart cards, email security, IP security, Time Stamp Protocol(TSP), web security, mobile communications, electronic commerce, Pay-TV etc., which links on many aspects of our daily lives.

In this paper, it has been developed an algorithm for cryptography in which we propose Laplace transforms for encrypting the plain text and corresponding inverse Laplace transforms for decryption.

General terms: *Encryption, Decryption, Plain Text, Cipher Text, Key.*

Keywords: *Laplace transforms, ASCII code, Network security, Cryptography.*

I. INTRODUCTION

The Laplace transform is a tool which consists many applications in numerous fields such as Electric circuit analysis, Communication systems, Hydrodynamics, Nuclear physics, Heat conduction, Wave equation, Solar systems, Signals and Systems. In this chapter, we are going to analyse and discuss Laplace transform application to cryptography.

Cryptography is an ancient subject, which is used as a security tool which hides information from hackers and safeguards the information from theft. This tool reached its maximum height at the time of first and second world wars. In the present scenario of excessive utilization and expansion of computer networks and the internet, the significance of network and computer data security is inevitable. Hence, the data should be secured from unauthorized usage and access which is a critical and imperative issue. So there is a greater need for security issues and cryptography is one of the most widely used paths for data security. The fundamental aspect of cryptography is to enable two sources to communicate over an insecure gateway in such a way that, the information would not be leaked or understood by any intruder in the basic process of communication. Encryption is the procedure of hiding required information and to make it unreadable and unavailable irrespective of special hacking knowledge. This process helps in maintaining secrecy and exclusively for private and personal communications. This Information can be secured and retained through the use of cryptography.

II. RELATED WORK

Encrypting and Decrypting process is carried forward using functional mathematical algorithms and secret keys in Trending cryptography. Mathematical techniques using matrices for encryption and decryption are found by Dhanorkar and Hiwarekar, Overbey, Traves and Wojdylo, Saeednia. Extensive work is also shown by Sachin & Bani in 2013 and by Swati Dhingra, Archana A.Savalgi and Swati Jain in 2016 by presenting new scheme for the cryptographic purpose by combining infinite series and Laplace transform using ASCII code. The process of encryption is further expanded using series expansion of f(t) and its Laplace transform. The Laplace transform is arranged in the form of an array with keys at even position, While the Decryption is done by inverse Laplace transforms. We use ASCII code along with hyperbolic cosine functions in this paper.

III. PROPOSED TECHNIQUE

The usage of Laplace transform has a wider perspective in many fields, including mathematics, physics and electrical engineering. This work proposes a new cryptographic scheme using Laplace transform which serves many transformations in security as per the requirement which is a useful factor for changing key where algorithm plays an important role. This, on the other hand directly makes it very difficult for an eyedropper to trace the key by any mode. The further usage of this application is carried forward in MATLAB and artificial neural network.

In the present paper a new cryptographic scheme is proposed using Laplace transform. The Laplace transform is used for encrypting the plain text and corresponding inverse Laplace transform is used for decryption. The Laplace transform is a generally used integral transform in mathematics, physics and electrical engineering that transforms a function of time into a function of complex frequency. The inverse Laplace transform takes a complex frequency domain function and gives a function defined in the time domain. Proposed algorithm serves as many transformations as per the requirements which are the better useful factor for changing key. Hence it is very difficult for an eyedropper to trace the key by any attack. The application has been done in MATLAB and artificial neural network. The expectation in such a problem clears and create forms of security which can prevent the hackers from attacking the information.

IV. DEFINITIONS AND STANDARD RESULTS

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.
Cipher text: When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.
Encryption and Decryption: It transforms a plain text message into cipher text, whereas decryption transforms a cipher text message back into plain text.

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

$$L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)\,dt \qquad (4.1)$$

provided that the integral exists. The corresponding inverse Laplace transform is

$$L^{-1}\{F(s)\} = f(t)\,. \qquad (4.2)$$

Here $f(t)$ and $F(s)$ are called as a combination of Laplace transforms.

2. Linearity Property: The Laplace transform is a linear transformation. The linearity property is stated as if $L\{f_1(t)\} = F_1(s)$, $L\{f_2(t)\} = F_2(s)$, then $L\{k_1 f_1(t) + k_2 f_2(t)\} = k_1 F_1(s) + k_2 F_2(s)$
Where c_1 and c_2 are constants.

3. Some Standard Results of Laplace Transform: In this paper, we are assuming that all the considered functions are such that their Laplace transform exists. Elementary functions include algebraic and transcendental functions.

1. $L\{t^n\} = \dfrac{n!}{s^{n+1}}$, $\qquad L^{-1}\left\{\dfrac{n!}{s^{n+1}}\right\} = t^n$, $n \in N$

2. $L\left\{t^n e^{kt}\right\} = \dfrac{n!}{(s-k)^{n+1}}$, $\qquad L^{-1}\left\{\dfrac{n!}{(s-k)^{n+1}}\right\} = t^n e^{kt}$

3. $L\{\cosh\ kt\} = \dfrac{s}{s^2 - k^2}$, $\quad s \geq |k|$

4. $L\left\{t^n f(t)\right\} = \left(\dfrac{-d}{ds}\right)^n F(s)$, $\qquad L^{-1}\left\{\left(\dfrac{-d}{ds}\right)^n F(s)\right\} = t^n f(t)$

V. PROPOSED METHODOLOGY

The following algorithm provides an insight into the proposed cryptographic scheme.
1. Method of Encryption:
Steps involved in Encryption as follows:
Step 1. Select the message, M to be sent, and convert into ASCII code. Let the length of the message be n.
Step 2. Let the given plain text is " ACADEMICS". Here n=9.
Based on the above step; ASCII code of plain text

A=65, C=67, A=65, D=68, E=69, M=77, I=73, C=67, S=83
Therefore, our plain text finite sequence is
G_0=65, G_1=67, G_2=65, G_3=68, G_4=69, G_5=77,
G_6=73, G_7=67, G_8=83, G_n=0 for $n \geq 9$.

Step 3. Writing these numbers as the coefficient in **tcoshrt** where r is a constant.
We consider standard expansion

$$\text{Coshrt} = 1 + \frac{r^2t^2}{2!} + \frac{r^4t^4}{4!} + \frac{r^6t^6}{6!} + \frac{r^8t^8}{8!} + \cdots + \frac{r^{2n}t^{2n}}{2n!} + \cdots = \sum_{n=0}^{\infty} \frac{(rt)^{2n}}{2n!} \qquad (5.1)$$

and

$$\text{tcoshrt} = t + \frac{r^2t^3}{2!} + \frac{r^4t^5}{4!} + \frac{r^6t^7}{6!} + \frac{r^8t^9}{8!} + \cdots + \frac{r^{2n}t^{2n+1}}{2n!} + \cdots = \sum_{n=0}^{\infty} \frac{r^{2n}t^{2n+1}}{2n!} \qquad (5.2)$$

Let us consider

$$f(t) = Gt \cosh 2t$$

$$= t\left\{G_0.1 + G_1\frac{2^2t^2}{2!} + G_2\frac{2^4t^4}{4!} + G_3\frac{2^6t^6}{6!} + G_4\frac{2^8t^8}{8!} + G_5\frac{2^{10}t^{10}}{10!} + G_6\frac{2^{12}t^{12}}{12!} + G_7\frac{2^{14}t^{14}}{14!} + G_8\frac{2^{16}t^{16}}{16!}\right\}$$

$$= 65t + 67\frac{t^3 2^2}{2!} + 65\frac{t^5 2^4}{4!} + 68\frac{t^7 2^6}{6!} + 69\frac{t^9 2^8}{8!} + 77\frac{t^{11} 2^{10}}{10!} + 73\frac{t^{13} 2^{12}}{12!} + 67\frac{t^{15} 2^{14}}{14!} + 83\frac{t^{17} 2^{16}}{16!}$$

$$= \sum_{n=0}^{\infty} \frac{G_n 2^{2n} t^{2n+1}}{2n!}$$

Step 4. Next, take the Laplace transform of a polynomial

$$L\{f(t)\} = L\{Gt \cosh 2t\}$$

$$= L\left\{65t + 67\frac{t^3 2^2}{2!} + 65\frac{t^5 2^4}{4!} + 68\frac{t^7 2^6}{6!} + 69\frac{t^9 2^8}{8!} + 77\frac{t^{11} 2^{10}}{10!} + 73\frac{t^{13} 2^{12}}{12!} + 67\frac{t^{15} 2^{14}}{14!} + 83\frac{t^{17} 2^{16}}{16!}\right\}$$

$$= \frac{65}{s^2} + \frac{804}{s^4} + \frac{5200}{s^6} + \frac{30464}{s^8} + \frac{158976}{s^{10}} + \frac{867328}{s^{12}} + \frac{3887104}{s^{14}} + \frac{16465920}{s^{16}} + \frac{92471296}{s^{18}}$$

Step 5. Next find r_i such that $r_i = M_i \bmod 200$ where i = 0, 1, 2, 3… n

r_0	=65 mod 200	= 200(0) +65	= 65
r_1	=804 mod 200	= 200(4) +4	= 4
r_2	=5200 mod 200	= 200(26) +0	= 0
r_3	=30464 mod 200	= 200(152) +64	= 64
r_4	=158976 mod 200	= 200(794) +176	= 176
r_5	=867328 mod 200	= 200(4336) +128	= 128
r_6	=3887104 mod 200	= 200(19435) +104	= 104
r_7	=16465920 mod 200	= 200(82329) +120	= 120
r_8	=92471296 mod 200	= 200(462356) +96	= 96

The ASCII values of above remainders will be the encrypted message.
Hence, the message ‘ACADEMICS’ is encrypted as ‘A♦@ÇhxՀ’

Step 6. Next find k_i such that $k_i = (M_i - r_i)/200$ where i=0,1,2,3,……n, and any denominator can be chosen.
Thus, key k_i is obtained as
k_0= 0, k_1= 4, k_2=26, k_3=152, k_4=794, k_5=4336, k_6=19435, k_7=82329, k_8=462356
Therefore, the cipher text is ‘A♦@ÇhxՀ’ and the key is 0, 4, 26, 152, 794, 4336, 19435, 82329,462356.

2. Method of Decryption:

Steps involved in Decryption as follows:

Step 1. Consider the cipher text and key received from the sender. In the above example cipher text is 'A♦@ÇhxŸ' and key is 0, 4, 26, 152, 794, 4336, 19435, 82329, 462356.

Step 2. Convert the given cipher text to a corresponding finite sequence of numbers, i.e. 65, 4, 0, 64, 176, 128, 104, 120, 96

Let

$G_0' = 65$, $G_1' = 4$, $G_2' = 0$, $G_3' = 64$, $G_4' = 176$, $G_5' = 128$, $G_6' = 104$, $G_7' = 120$, $G_8' = 96$

Step 3. The given key k_i for i = 0, 1, 2…n as 0, 4, 26, 152, 794, 4336, 19435, 82329, 462356.

Let $M_i = 200ki + G_i'$ for i=0, 1, 2, 3……

$M_0 = 200(0) + 65 = 65$ $M_5 = 200(4336) +128 = 867328$

$M_1 = 200(4) + 4 = 804$ $M_6 = 200(19435) +104 = 3887104$

$M_2 = 200(26) +0 = 5200$ $M_7 = 200(82329) +120 = 16465920$

$M_3 = 200(152) +64 = 30464$ $M_8 = 200(462356) +96 = 92471296$

$M_4 = 200(794) +176 = 158976$

Now we consider

$$G\left\{\frac{-d}{ds}\right\}\frac{s}{\left(s^2-2^2\right)}$$

$$=\frac{65}{s^2}+\frac{804}{s^4}+\frac{5200}{s^6}+\frac{30464}{s^8}+\frac{158976}{s^{10}}+\frac{867328}{s^{12}}+\frac{3887104}{s^{14}}+\frac{16465920}{s^{16}}+\frac{92471296}{s^{18}}$$

$$=\sum_{n=0}^{\infty}\frac{M_n}{s^{2n+2}}$$

Step 4. Now take Inverse Laplace transform of a polynomial, we get

$$f(t) = Gt\ \cosh\ 2t$$

$$= L^{-1}\left\{\frac{65}{s^2}+\frac{804}{s^4}+\frac{5200}{s^6}+\frac{30464}{s^8}+\frac{158976}{s^{10}}+\frac{867328}{s^{12}}+\frac{3887104}{s^{14}}+\frac{16465920}{s^{16}}+\frac{92471296}{s^{18}}\right\}$$

$$= 65\,t + 67\,\frac{t^3 2^2}{2!} + 65\,\frac{t^5 2^4}{4!} + 68\,\frac{t^7 2^6}{6!} + 69\,\frac{t^9 2^8}{8!} + 77\,\frac{t^{11} 2^{10}}{10!} + 73\,\frac{t^{13} 2^{12}}{12!} + 67\,\frac{t^{15} 2^{14}}{14!} + 83\,\frac{t^{17} 2^{16}}{16!}$$

Hence, we have

G_0=65, G_1=67, G_2=65, G_3=68, G_4=69, G_5=77,

G_6=73, G_7=67, G_8=83, G_n=0 for $n \geq 9$

Step 5. Now, convert the numbers of above finite sequence to alphabets (ASCII values), the original plain text is obtained as "ACADEMICS"

VI. RESULTS AND DISCUSSION

1. Input-Output

Use of Laplace Transformation in Encryption

The input given to the encryption algorithm is

Plain Text: ACADEMICS

The output obtained after encryption is

Cipher Text: A♦@ÇhxŸ

The Key used for Decryption is

0, 4, 26, 152, 794, 4336, 19435, 82329,462356.

Use of Inverse Laplace Transform in Decryption

The input given to the decryption algorithm is

Cipher Text: A♦@ÇhxŸ

The output obtained after decryption is

Plain Text: ACADEMICS

VII. GENERALIZATION OF THE RESULT

Generalized functions of section (V) are extended with the required results. For encryption of the given message in terms of G_i .

We consider

$f(t) = Gt^{j} \cosh rt$, $r, j \in N$ (the set of Natural numbers).

Taking the Laplace transform of $f(t)$ and follow the procedure as discussed in section 5, the given message can be converted from G_i to $G_i^{'}$ where

$G_i^{'} = G_i r^{2i}(2i+1)(2i+2)....(2i+j) \bmod 200 = q_i \bmod 200$

Where $q_i = G_i r^{2i}(2i+1)(2i+2)....(2i+j)$, i = 0,1,2,3, ……., with a key

$$k_i = \frac{q_i - G_i^{'}}{200} \text{ for i} = 0,1,2,3,\ldots\ldots$$

For decryption of a received message in terms of $G_i^{'}$ we consider

$$G\left\{\frac{-d}{ds}\right\}^{j} \frac{s}{\left(s^2 - r^2\right)} = \sum_{n=0}^{\infty} \frac{q_n}{s^{2n+j+1}} .$$

Taking the inverse Laplace transform and using the procedure discussed in section 5, we can convert given message string $G_i^{'}$ to G_i where

$$G_i = \frac{200\ k_i + G_i^{'}}{r^{2i}(2i+1)(2i+2).....(2i+j)}, \quad \text{i} = 0,1,2,3\ldots$$

VIII. ILLUSTRATIVE EXAMPLES

We have the original message

1. ‘ACADEMICS’ gets converted to ‘A○}♦╡gm-é’ with key as
0, 9, 131, 1735, 20371, 250072, 2521687, 24034419, 303694616, for r = 3.
2. ‘ACADEMICS’ gets converted to ‘A►`8H┤’ with key as
0, 16, 416, 9748, 203489, 4440719, 79607889, 1348888167, 30300994280, for r = 4.
3. ‘ACADEMICS’ gets converted to ‘A↓}d}»d’ with key as
0, 25, 1015, 37187, 1212890, 41357421, 1158447265, 30670166020, 1076507569000, for r = 5.

IX. CONCLUSIONS

1. In the proposed work we expand an innovative cryptographic scheme using Laplace transforms of hyperbolic functions using ASCII code and the key is the number of multiples of mod n. projected algorithm provides many transformations as per the requirements which are the most functional factor for changing key. Therefore, it is very tricky for an eyedropper to trace the key by any attack.
2. The similar results can be obtained by using the Laplace transform of some other suitable functions. Hence, extension of this work is possible.
3. Several sectors such as banking and other financial institutions are adopting e-services and improving their Internet services. However, the e-service necessities are also opening up new chance to propagate financial fraud. Internet banking fraud is one of the most severe electronic crimes and mostly committed by unofficial and illegal users.
4. To reduce the crypt -analysis attack risk, a powerful key theory plays vital role in the method presented in this paper is useful in such situations.

ACKNOWLEDGEMENT

Authors are thankful to Vignana Bharathi Institute of Technology, Aushapur (V), Ghatkesar (M), Medchal Dist, Telangana, India, for the support to this work.

REFERENCES

[1] Alexander Stanoyevitch, Introduction to cryptography with mathematical foundations and computer implementations, CRC Press, (2002).
[2] Barr T.H., Invitation to Cryptography, Prentice Hall, 2002.
[3] Blakley G.R., Twenty years of Cryptography in the open literature, Security and Privacy, Proceedings of the IEEE Symposium, May 1999, 9 -12.
[4] Eric C., Ronald K . and James W.C., Network Security Bible, Second edn., Wiley India pub., 2009.
[5] Erwin Kreyszing, Advanced Engineering Mathematics, John Wiley and Sons Inc., 1999.
[6] G.Naga Lakshmi, Ravi Kumar B. and Chandra Sekhar A., A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2, 2011, 2515-2519.
[7] Grewal B.S., Higher Engineering Mathematics, Khanna Pub., Delhi, 2005.
[8] Hiwarekar A.P., A new method of cryptography using Laplace transform of hyperbolic functions, International Journal of Mathematical Archive- 4(2), 2013, 208-213.
[9] Hiwarekar A.P., Application of Laplace Transform for Cryptographic Scheme, proceeding of World Congress on Engineering Vol.II, LNCS, 2013, 95-100.
[10] Johannes A. Buchmann, Introduction to Cryptography, Fourth Edn., Indian Reprint, Springer, 2009.
[11] Overbey J., Traves W. and Wojdylo J., On the Key space of the Hill Cipher, Cryptologia, 29(1), January 2005, 59-72.
[12] Saeednia S., How to Make the Hill Cipher Secure, Cryptologia, 24(4), October 2000, 353-360.
[13] Stallings W., Cryptography and network security, 4th edition, Prentice Hall, 2005.
[14] Stallings W., Network security essentials: Applications and standards, first edition, Pearson Education, Asia, 2001.
[15] Sukalyan Som and Moumita Som., Article: DNA Secret Writing with Laplace Transform, International Journal of Computer Applications, July 2012, 50(5):44-50.
[16] Swati Dhingra, Archana A. Savalgi and Swati Jain, Laplace Transformation based Cryptographic Technique in Network Security, International Journal of Computer Applications, Volume 136, No.7, February 2016, 0975-8887.