Laplace Transformation based Cryptographic Technique in Network Security

Swati Dhingra
VIT University

Archana A. Savalgi
VIT University

Swati Jain
VIT University

ABSTRACT
Information security has been an essential part of human life from old time. In computer society, information protection turns out to be more vital for humankind and new rising technologies are developing in a perpetual stream. Cryptography is one of the most important techniques used for securing transmission of messages and protection of data. It provides privacy and security for the secret information by hiding it from unauthorized users.

In this paper authors have proposed a method of cryptography, in which authors have used Laplace transform for encrypting the plain text and corresponding inverse Laplace transform for decryption. This paper is based on the work of [1,2,3,4].

General Terms
Encryption, Decryption, Plain Text, Cipher Text, Key

Keywords
Laplace Transform, Network Security, Cryptography

1. INTRODUCTION
In Today's world, with expanding utilization of computer networks and internet, the significance of network, computer and data security is self driven. To be secured, data should be shielded from unauthorized access. Hence, data security has become a critical and imperative issue. One of the widely used methodologies for data security is cryptography.

Cryptography, the mathematic of encryption, plays a indispensable part in numerous fields. Cryptography is the only most important tool that avoids the threat against possible attacks by hackers during transmission process of the message. 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 [5,6].

2. RELATED WORK
Modern cryptography uses sophisticated mathematical equations (algorithms) and secret keys to encrypt and decrypt data. Various techniques for cryptography are found in **literature [7],[8],[9],[10],[11],[12],[13]. Mathematical** technique using matrices for the same are found in Dhanorkar and Hiwarekar,[14]; Overbey, Traves and Wo-jdylo,[15];Saeednia,[16].In 2013 Sachin & Bani presented different scheme for cryptographic purpose, by combining Infinite series and Laplace transform using ASCII code (128 bit). Encryption is done by using Infinite series and then Laplace transform, arranged in the form of an array with keys at even position. Decryption is done by inverse Laplace transform. In Naga Lakshmi, Ravi Kumar and Chandra Sekhar,[2]; Hi-warekar,[3] and [4]; they encrypt a string by using series expansion of *f(t)* and its Laplace transform. Here in this paper authors have used Laplace transform for cryptography.

3. PROPOSED TECHNIQUE
In the present paper a new cryptographic scheme is proposed using Laplace Transform. Laplace transform is used for encrypting the plain text and corresponding inverse Laplace transform is used for decryption. The Laplace transform is a widely used integral transform in mathematics 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 yields a function defined in the time domain. Proposed algorithm provides as many transformations as per the requirements which are the most useful factor for changing key. Therefore it is very difficult for an eyedropper to trace the key by any attack. The implementation has been done in MATLAB.

4. DEFINITIONS AND STANDARD RESULTS
Definition 4.1 Plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

Definition 4.2 When plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

Definition 4.3 Encryption transforms a plain text message into cipher text, whereas decryption transforms a cipher text message back into plain text.

Every encryption and decryption process has two aspects: The algorithm and the key. The key is used for encryption and decryption that makes the process of cryptography secure. Here authors require following results [1].

4.1. Laplace Transforms
Laplace Transforms involve two domains : (1) the time domain in which the signal is represented by its waveform *f(t)*, and (2) the frequency domain in which the signal is characterized by its transform.

If *f(t)* is a function defined for all positive values of t, then the Laplace transform of *f(t)* is defined as

$$\mathcal{L}\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)dt \qquad (1)$$

provided that the integral exists. Here the parameter *s* is a real or complex number. The corresponding inverse Laplace transform is

$$\mathcal{L}^{-1}\{F(s)\} = f(t) \qquad (2)$$

Here *f(t)* and *F(s)* are called as pair of Laplace transforms.

4.2. Linearity Property

Laplace transform is a linear transformation which means that the transform of a sum of waveforms is the sum of their transforms. Stated formally the linearity property is

$$\mathcal{L}\{Af_1(t) + Bf_2(t)\} = AL_1(s) + BL_2(s) \quad (3)$$

where A and B are constants.
The above result can easily be generalized to more than two functions.

4.3. Laplace Transforms of Elementary Functions

Elementary functions include algebraic and transcendental functions.

$$\mathcal{L}\{t^n\} = \frac{n!}{s^{n+1}}, \qquad \mathcal{L}^{-1}\left\{\frac{n!}{s^{n+1}}\right\} = t^n \quad (4)$$

$$\mathcal{L}\{te^t\} = \frac{1}{(s-k)^2}, \ \mathcal{L}^{-1}\left\{\frac{1}{(s-k)^2}\right\} = te^{kt} \quad (5)$$

5. PROPOSED METHODOLOGY

The following algorithm provides an insight into the proposed cryptographic scheme. The sender converts the original message or plain text into cipher text using the following steps.

Method of Encryption

I. Select the message, M, to be sent, and convert into ASCII code. Let length of message be *n*.

II. The plain text message is organized as a finite sequence of numbers, based on the above conversion. For example our plain text is "HELLOWORLD". Here n=10.

Based on the above step; ASCII code of pain text
H=72, E=69, L=76, L=76, O=79, W=87, O=79, R=82, L=76, D=68

Therefore our plain text finite sequence is
Let
G_0=72, G_1=69, G_2=76, G_3=76, G_4=79, G_5=87, G_6=79, G_7= 82, G_8= 76, G_9=68, G_n=0 *for n≥10*

III. Writing these numbers as the coefficient in $\mathbf{t\,e^{rt}}$ where r is a constant.

Authors consider standard expansion

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

and (6)

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

(7)

where r is a constant

Let us consider

$$f(t) = Gte^{2t}$$

$$= t[G_0.1 + G_1.\frac{2t}{1!} + G_2.\frac{2^2t^2}{2!} + G_3.\frac{2^3t^3}{3!} + G_4.\frac{2^4t^4}{4!} + G_5.\frac{2^5t^5}{5!} + G_6.\frac{2^6t^6}{6!} + G_7.\frac{2^7t^7}{7!} + G_8.\frac{2^8t^8}{8!} + G_9.\frac{2^9t^9}{9!}]$$

$$= 72.t + 69.\frac{2t^2}{1!} + 76.\frac{2^2t^3}{2!} + 76.\frac{2^3t^4}{3!} + 79.\frac{2^4t^5}{4!} + 87.\frac{2^5t^6}{5!} + 79.\frac{2^6t^7}{6!} + 82.\frac{2^7t^8}{7!} + 76.\frac{2^8t^9}{8!} + 68.\frac{2^9t^{10}}{9!}$$

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

IV. Next take Laplace transform of a polynomial

$$F(s) = \mathcal{L}\big((f(t),s\big) = \mathcal{L}\{t[G_0.1 + G_1\frac{2^1t}{1!} + G_2\frac{2^2t}{2!} + G_3\frac{2^3t}{3!} + G_4\frac{2^4t}{4!} + G_5\frac{2^5t}{5!} + G_6\frac{2^6t}{6!} + G_7.\frac{2^7t^8}{7!} + G_8.\frac{2^8t^9}{8!} + G_9.\frac{2^9t^{10}}{9!})]\}$$

$$= \mathcal{L}(72.t + 69.\frac{2t^2}{1!} + 76.\frac{2^2t^3}{2!} + 76.\frac{2^3t^4}{3!} + 79.\frac{2^4t^5}{4!} + 87.\frac{2^5t^6}{5!} + 79.\frac{2^6t^7}{6!} + 82.\frac{2^7t^8}{7!} + 76.\frac{2^8t^9}{8!} + 68.\frac{2^9t^{10}}{9!})$$

$$= \frac{72}{s^2} + \frac{276}{s^3} + \frac{912}{s^4} + \frac{2432}{s^5} + \frac{6320}{s^6} + \frac{16704}{s^7} + \frac{35392}{s^8} + \frac{83968}{s^9} + \frac{175104}{s^{10}} + \frac{348160}{s^{11}}$$

V. Next find r_i such that $r_i = F_i \ mod\ 200$ where *i=0,1,2,3...n*

r_0	$=72\ mod\ 200$	=72
r_1	$=276 mod\ 200$	=76
r	$=912\ mod\ 200$	=112
r_3	$=2432\ mod\ 200$	=32
r_4	$=6320\ mod\ 200$	=120
r_5	$=1670\ mod\ 200$	=104
r_6	$=35392 mod\ 200$	=192
r_7	$=83968\ mod\ 200$	=168
r_8	$=175104 mod\ 200$	=104
r_9	$=348160\ mod\ 200$	=160

The ASCII values of above remainders will be the Encrypted message.
Hence the message 'HELLOWORLD' is encrypted as
'HLp xhÀ¨h'

VI. Next find k_i such that $k_i = (F_i - r_i)/200$ 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=1, k_2=4, k_3=12, k_4=31, k_5=83, k_6=176, k_7=419, k_8=875, k_9= 1740
Therefore, the cipher text is 'HLp xhÀ¨h' and key is 0, 1, 4, 12, 31, 83, 176, 419, 875, 1740

Method of Decryption

I. Consider the cipher text and key received from sender. In the above example cipher text is 'HLp xhÀ¨h' and key is 0, 1, 4, 12, 31, 83, 176, 419, 875, 1740.

II. Convert the given cipher text to corresponding finite sequence of numbers

i.e. 72, 76, 112, 32, 120, 104, 192, 168, 104, 160

Let
G'_0=72, G'_1=76, G'_2=112, G'_3=32, G'_4=120, G'_5=104, G'_6=192, G'_7= 168, G'_8= 104, G'_9=160

III. Using given key k_i for i=0,1,2... as 0 1 4 12 31 83 176 419 875 1740 and assuming

$$F_i = 200k_i + G'_i \quad for\ i=0,1,2,3...$$

$F_{0=}$ 200*0 +72= 72 $F_{1=}$ 200*1 +76=276
$F_{2=}$200*4 +112=912 $F_{3=}$200*12 +32=2432
$F_{4=}$200*31 +120=6320 $F_{5=}$200*83 +104=16704
$F_{6=}$200*176 +192=35392 $F_{7=}$200*419 +168=83968
$F_{8=}$200*875 +104=175104 $F_{9=}$200*1740 +160=348160

Now consider

$$G\frac{1}{(s-2)^2} = \frac{72}{s^2}+\frac{276}{s^3}+\frac{912}{s^4}+\frac{2432}{s^5}+\frac{6320}{s^6}+\frac{16704}{s^7}+\frac{35392}{s^8}+\frac{83968}{s^9}+\frac{175104}{s^{10}}+\frac{348160}{s^{11}}$$

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

IV. Next take Inverse Laplace transform of a polynomial

$$f(t) = Gte^{2t} = \mathcal{L}^{-1}\{\frac{72}{s^2}+\frac{276}{s^3}+\frac{912}{s^4}+\frac{2432}{s^5}+\frac{6320}{s^6}+\frac{16704}{s^7}+\frac{35392}{s^8}+\frac{83968}{s^9}+\frac{175104}{s^{10}}+\frac{348160}{s^{11}}\}$$

$$= 72.t + 69.\frac{2t^2}{1!} + 76.\frac{2^2t^3}{2!} + 76.\frac{2^3t^4}{3!} + 79.\frac{2^4t^5}{4!} + 87.\frac{2^5t^6}{5!} + 79.\frac{2^6t^7}{6!} + 82.\frac{2^7t^8}{7!} + 76.\frac{2^8t^9}{8!} + 68.\frac{2^9t^{10}}{9!}$$

V. Consider the coefficients of a polynomial *f(t)* as finite sequence
Here,
G_0=72, G_1=69, G_2=76, G_3=76, G_4=79, G_5=87, G_6=79, G_7= 82, G_8= 76, G_9=68

VI. Now, translating the numbers of above finite sequence to alphabets(ASCII values), original plain text is obtained as 'HELLOWORLD'

6. RESULTS AND DISCUSSION

6.1 Input-Output

Encryption using Laplace Transformation
The input given to the encryption algorithm is-
Plain Text: HELLOWORLD
The output obtained after encryption is-
Cipher Text : HLp xhÀ¨h
Key used for Decryption is
0, 1, 4, 12, 31, 83, 176, 419, 875, 1740

Decryption using Inverse Laplace Transform
The input given to the decryption algorithm is-
Cipher Text : HLp xhÀ¨h
The output obtained after decryption is-
Plain Text: HELLOWORLD

6.2 Encryption and Decryption Time

Encryption and Decryption time with respect to different input sizes have been presented in table 1 accompanied by corresponding graph as presented in Fig It is revealed as input size increases, encryption and decryption time increases. Also, encryption time is more compared to decryption time.

Table 1. Encryption/Decryption Time(ms) v/s Input Length

Input Length	Encryption Time	Decryption Time
10	0.9606	0.4190
20	1.1785	0.6272
30	1.5144	0.8699
40	1.8273	1.0420
50	2.1086	1.2312

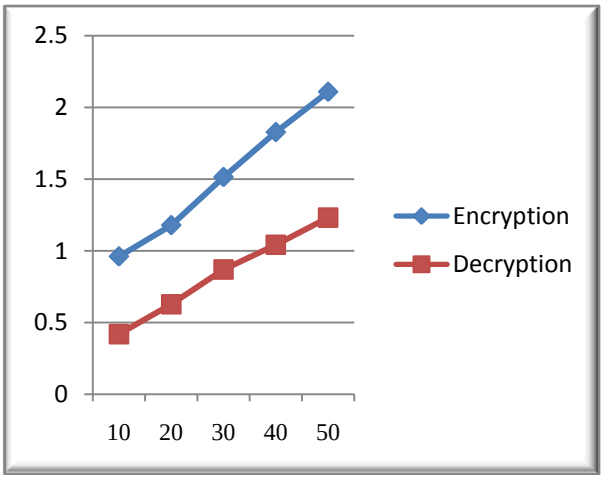

Fig 2: Encryption/Decryption Time(ms) v/s Input Length

7. GENERALIZATION OF THE RESULT

For encryption of given message in terms of G_i, consider $f(t)=Gte^{rt}$, r$\in$N, where N is the set of natural numbers. Taking Laplace transform and follow the procedure discussed

in chapter 3, then given message can be converted from G_i to G'_i

Where $G'_i = G_i r^i (i+1) \bmod 200 = q_i \bmod 200$

where $q_i = G_i r^i (i+1)$ i=0,1,2… with key $k_i = \frac{q_{i-G'_i}}{200}$

for i=0,1,2,3… For decryption of received message in terms of G'_i 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, given received message can be converted from G'_i to G_i where $G_{i=\frac{200k_i+G'_i}{r^i(i+1)}}$ i=0,1,2…

8. ILLUSTRATIVE EXAMPLE

Original message obtained is

a. 'HELLOWORLD' gets converted to 'H 4Ã. H|(' with key as
   0, 2, 10, 41, 159, 634, 2015, 7173, 22438, 66922, for r = 3
b. 'HELLOWORLD' gets converted to 'H|¬HÃ6aT' with key as
   0, 4, 55, 521, 4741, 43866, 325299, 2701221, 19715619, 137202263, for r = 7
c. 'HELLOWORLD' gets converted to 'HTH x`HÀ,(' with key as
   0, 12, 369, 8864, 207327, 4931772, 94043799, 2008081704, 37688265169, 67442158725, for r =18

9. APPLICATIONS

a. A symmetric key cryptographic system termed as DSWLT. This procedure is quick, suitable for encryption of huge records. DSWLT consider the plain text (i.e. the input file) as binary string with limited no of bits. The input string converted to DNA nucleotides using DNA coding and then the DNA codes are converted to positive integers. Laplace transform is applied considering these numbers to be the co-efficient of the expansion. To provide multilevel security the resultant coefficients are converted to their binary equivalent and another level of encryption with cumulative XOR is performed and respective MSBs found at every iteration are taken to construct the cipher text. Decryption is performed in the opposite manner [17].

b. Mobile adhoc network is collection of autonomous nodes that are frequently moving without the centralized control. Mobile adhoc networks are multi hop wireless networks without fixed infrastructure. Node frequently change topology, due to this type of behavior transformation of information from one node to another node is more complicated task. Decentralized nature of mobile adhoc network is more vulnerable to attack like denial of service (DOS) which consumes more bandwidth and resources. Security is major concern in adhoc network, so in this paper, Lagrange polynomial and Laplace transform and inverse Laplace transform to enhance secure communication for MANET [18].

c. The proposed technique can be used in Message Passing(Coding Theory) in which the exchange of messages is administered in a confidential and more secured way having a wide application in Military operations, Banking Transactions etc

10. CONCLUSION

a. Cryptography is one of the first lines of defense against hackers and crackers in today's world. Thus, it will stay important for a long time to come.
b. Many sectors such as banking and other financial institutions are adopting e-services and improving their internet services. However, the e-service requirements are also opening up new opportunity to commit financial fraud. Internet banking fraud is one of the most serious electronic crimes and mostly committed by unauthorized users.
c. In the proposed work authors develop a new cryptographic scheme using Laplace transform. The proposed algorithm is simple, straight forward but intrinsically strong and compact approach to cryptography. It provides the same or sometimes even better level of security using minimal time complexity.
d. The new method of key generation scheme which is entirely based on the input given, developed in this paper may be used for a fraud prevention mechanism. Proposed algorithm provides as many transformations as per the requirements which are the most useful factor for changing key. Therefore it is very difficult for an eyedropper to trace the key by any attack.
e. The similar results can be obtained by using Laplace transform of other suitable function. Hence extension of this work is possible.
f. Encryption and Decryption time with respect to different input sizes has been calculated. It is revealed that as input size increases, encryption and decryption time increases. Also, encryption time is more compared to decryption time.

11. REFERENCES

[1] A.P.Hiwarekar, Application of Laplace Transform For Cryptographic Scheme, Proceedings of the World Congress on Engineering 2013 Vol I, WCE 2013, July 3 - 5, 2013, London, U.K.

[2] G.Naga Lakshmi, B.Ravi Kumar and A.Chandra Sekhar, A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2, 2515-2519, (2011).

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

[4] Hiwarekar A.P., A new method of cryptography using Laplace transform of hyperbolic functions, International Journal of Mathematical Archive,4(2),208-213,(2013).

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

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

[7] Alexander Stanoyevitch, Introduction to cyrptography with mathematical foundations and computer implementations, CRC Press, (2002).

[8] Barr T.H., Invitation to Cryptography, Prentice Hall, (2002).

[9] Blakley G.R., Twenty years of Cryptography in the open literature, Security and Privacy 1999, Proceedingsof the IEEE Symposium, 9-12, (May1999).

[10] Eric C., Ronald K., James W.C., Network Security Bible Second edn., Wiley India pub.(2009).

[11] Johannes A. Buchmann, Introduction to Cryptography, Fourth Edn., Indian Reprint ,Springer,(2009).

[12] Stallings W., Cryptography and network security, 4th edition, Prentice Hall, (2005).

[13] Stallings W., Network security essentials: Applications and standards,first edition, Pearson Education, Asia, (2001).

[14] 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, 19-23, (July 2011).

[15] Overbey J., Traves W.and Wojdylo J., On the Keyspace of the Hill Cipher, Cryptologia, 29, 59-72, (January 2005).

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

[17] Sukalyan Som and Moumita Som. Article: DNA Secret Writing with Laplace Transform. International Journal of Computer Applications 50(5):44-50, (July 2012).

[18] Sumee Rai, Nidhi Tyagi and Pradeep Kumar. Article:Secure communication for mobile Adhoc network using(LPIT) Lagrange polynomial and Integral transform with Exponential Function. International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1 Issue 6 (July 2014)