RESEARCH ARTICLE OPEN ACCESS

Cryptography Using Laplace Transform

A.P. Hiwarekar
Department of Mathematics Vidya Pratishthan's College of Engineering Baramati (University of Pune)
Vidyanagari, Bhigwan Road, Baramati, Dist.Pune, Maharashtra, India

Abstract
In this paper we present a new iterative method for cryptography, in which we apply Laplace transform of suitable function for encrypting the plain text and we apply corresponding inverse Laplace transform for decryption. Finally we developed the results in the generalized form. We also obtained the corresponding encryption algorithm for this method.

Keywords: Cryptography, Data encryption, Applications to coding, coding theory and cryptography, Algebraic coding theory; cryptography, Laplace Transforms.

I. Introduction

When we send a message to someone, we always suspect that someone else will interpret it and read it or modify it before re-sending. There is always a desire to know about a secret message being sent or received between two parties with or without any personal, financial or political gains. It is no wonder that to have the desire to send a message to someone so that nobody else can interpret it. Thus information security has become a very critical aspect of modern computing system. Information security is mostly achieved through the use of cryptography.

Various techniques for cryptography are found in literature [1], [2], [3], [4], [12], [17], [18]. Mathematical technique using matrices for the same are found in Overbey, Traves and Wojdylo, [14]; Saeednia, [16]. In Naga Lakshmi, Ravi Kumar and Chandra Sekhar, [6]; Hiwarekar, [8], [9], [10] and [11]; they encrypt a string by using series expansion of $f(t)$ and its Laplace transform.

II. Definitions and Standard Results

Definition 2.1.: 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 2.2.: When plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

Definition 2.3.: 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 we require following results.

2.1. 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

$$L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)dt, \qquad (2.1)$$

provided that the integral exists. Here the parameter s is a real or complex number. The corresponding inverse Laplace transform is $L^{-1}\{F(s)\} = f(t),$ [5, 13, 15].

2.2. Theorem: Laplace transform is a linear transform. That is, if

$$L\{f_1(t)\} = F_1(s), L\{f_2(t)\} = F_2(s), \cdots L\{f_n(t)\} = F_n(s), \qquad (2.2)$$

then

$$L\{c_1 f_1(t) + c_2 f_2(t) + \cdots c_n f_n(t)\} = c_1 F_1(s) + c_2 F_2(s) + \cdots + c_n F_n(s), \qquad (2.3)$$

where $c_1, c_2, \cdots, c_n$ are constants, [5, 13, 15].

2.3. Some Standard Results of Laplace Transform:
In this paper we are assuming that all the considered functions are such that their Laplace transform exists. We are also assuming that N be the set of natural numbers. Here we require following standard results of Laplace transform

1. $L\{\cosh kt\} = \dfrac{s}{s^2 - k^2}, \quad L^{-1}\{\dfrac{s}{s^2 - k^2}\} = \cosh kt.$ (2.4)
2. $L\{t^n\} = \dfrac{n!}{s^{n+1}}, \quad L^{-1}\{\dfrac{n!}{s^{n+1}}\} = t^n, \quad n \in N.$ (2.5)
3. $L\{t^n f(t)\} = \left(\dfrac{-d}{ds}\right)^n F(s), \quad L^{-1}\{\left(\dfrac{-d}{ds}\right)^n F(s)\} = t^n f(t),$ (2.6)

[5, 13, 15].

III. MAIN RESULTS

3.1 Encryption

We consider standard expansion

$$\cosh rt = 1+\frac{r^2t^2}{2!}+\frac{r^4t^4}{4!}+\frac{r^6t^6}{6!}+\cdots+\frac{r^{2i}t^{2i}}{2i!}+\cdots+\cdots=\sum_{i=0}^{\infty}\frac{(rt)^{2i}}{2i!}, \tag{3.1}$$

where $r \in N$ is a constant, and

$$t^2\cosh 2t = t^2+\frac{2^2t^4}{2!}+\frac{2^4t^6}{4!}+\frac{2^6t^8}{6!}+\cdots+\frac{2^{2i}t^{2i+2}}{2i!}+\cdots+\cdots$$
$$=\sum_{i=0}^{\infty}\frac{2^{2i}t^{2i+2}}{2i!}. \tag{3.2}$$

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

Let given message called plain text be ‘FRUITS’, it is equivalent to

5 17 20 8 19 18.

Let us assume that

$G_{0,0}=5,\quad G_{1,0}=17,\quad G_{2,0}=20,\quad G_{3,0}=8,\quad G_{4,0}=19,\quad G_{5,0}=18,\quad G_{n,0}=0$ for n ≥ 6.

Writing these numbers as a coefficients of $t^2\cosh 2t,$ and assuming $f(t)=Gt^2\cosh 2t,$ we get

$$f(t)=t^2[G_{0,0}+G_{1,0}\frac{2^2t^2}{2!}+G_{2,0}\frac{2^4t^4}{4!}+G_{3,0}\frac{2^6t^6}{6!}+G_{4,0}\frac{2^8t^8}{8!}+G_{5,0}\frac{2^{10}t^{10}}{10!}]$$

$$=\sum_{i=0}^{\infty}\frac{2^{2i}t^{2i+2}G_{i,0}}{2i!}=5\frac{t^2}{0!}+17\frac{2^2t^4}{2!}+20\frac{2^4t^6}{4!}+8\frac{2^6t^8}{6!}+19\frac{2^8t^{10}}{8!}+18\frac{2^{10}t^{12}}{10!}. \tag{3.3}$$

Taking Laplace transform on both sides of (3.3), we have

$$L\{f(t)\}=L\{Gt^2\cosh 2t\}=\frac{10}{s^3}+\frac{816}{s^5}+\frac{9600}{s^7}+\frac{28672}{s^9}+\frac{437760}{s^{11}}+\frac{2433024}{s^{13}}. \tag{3.4}$$

Adding $p=10$ to the resultant values 10 816 9600 28672 437760 2433024 and then adjusting it to mod 26 that is

$$20 = 20 \bmod 26,\qquad 826 = 20 \bmod 26,\qquad 9610 = 16 \bmod 26,$$
$$28682 = 4 \bmod 26,\qquad 437770 = 8 \bmod 26,\qquad 2433034 = 6 \bmod 26.$$

Sender sends the values

0 31 369 1103 16837 93578

as a key. Assuming

$G_{0,1}=20,\quad G_{1,1}=20,\quad G_{2,1}=16,\quad G_{3,1}=4,\quad G_{4,1}=8\quad G_{5,1}=6,$

$G_{n,1}=0$ for n ≥ 6.

The given plain text gets converted to cipher text

20 20 16 4 8 6.

Here message ‘FRUITS’ gets converted to ‘UUQEIG’. These results are included in the following

Theorem 3.1: The given plain text in terms of $G_{i,0},\ i=1,2,3,\cdots,$ *under Laplace transform of* $Gt^2\cosh 2t,$ *(that is by writing them as a coefficients of* $t^2\cosh 2t,$ *and then taking the Laplace transform) can be converted to cipher text*

$$G_{i,1}=(2^{2i}(2i+1)(2i+2)G_{i,0}+p)\bmod 26$$
$$=q_{i,1}-26k_{i,1},\quad for\ i=0,1,2,3,\cdots, \tag{3.5}$$

where,

$$q_{i,1}=2^{2i+1}(2i+1)(2i+2)G_{i,0}+p,\ \ i=0,1,2,3,\cdots,p\in N,\quad 0\le p\le 25, \tag{3.6}$$

and a key

$$k_{i,1}=\frac{q_{i,1}-G_{i,1}}{26}\quad for\ \ i=0,1,2,3,\cdots. \tag{3.7}$$

Now we apply the same operation again on the output of the resulting cipher text obtained in the Theorem 3.1 and obtain its new form which is included in the following theorem.

Theorem 3.2: The given plain text in terms of $G_{i,1},\ i=1,2,3,\cdots,$ *under Laplace transform of* $G_{i,1}t^2\cosh 2t,$ *(that is by writing them as a coefficients of* $t^2\cosh 2t$ *and then taking the Laplace transform) can be converted to cipher text*

$$G_{i,2}=(G_{i,1}2^{2i}(2i+1)(2i+2)+p)\bmod 26=q_{i,2}-26k_{i,2},\ \ i=0,1,2,3,\cdots, \tag{3.8}$$

where,

$$q_{i,2}=(G_{i,1}2^{2i}(2i+1)(2i+2)+p),\ i=0,1,2,3,\cdots,p\in N,\quad 0\le p\le 25, \tag{3.9}$$

and a key

$$k_{i,2}=\frac{q_{i,2}-G_{i,2}}{26},\ i=0,1,2,3,\cdots,. \tag{3.10}$$

Now we apply such operations successively j times on the given plain text and obtain its new form as cipher text. This iterative method is included in the following theorem.

Theorem 3.3: The given plain text in terms of $G_{i,0},\ i=1,2,3,\cdots,$ *under Laplace transform of* $G_{i,0}t^2\cosh 2t,$ *successively j times (that is by writing them as a coefficients of* $t^2\cosh 2t,$ *and then taking the Laplace transform successively) can be converted to cipher text*

$$G_{i,j}=(G_{i,j-1}\ 2^{2i+1}(2i+1)(2i+2)+p)\ \bmod 26=q_{i,j}-26k_{i,j},\ i,j=0,1,2,3,\cdots, \tag{3.11}$$

where

$$q_{i,j}=(G_{i,j-1}2^{2i}(2i+1)(2i+2)+p),\ i,j=0,1,2,3,\cdots,\ p\in N,\quad 0\le p\le 25, \tag{3.12}$$

and a key

$$k_{i,j}=\frac{q_{i,j}-G_{i,j}}{26},i,\ j=0,1,2,3,\cdots, \tag{3.13}$$

Remark 3.1: Theorem 3.1 is a special case of Theorem 3.3 with $j = 1$ and Theorem 3.2 with $j = 2$.

Remark 3.2: Results in [10], Hiwarekar A.P are generalized here and are special cases of Theorem 3.3 with $j = 1$ and with $p = 0$.

3.2. Generalization

The generalization of the results in section 3 can be obtained by considering more general function given by $f(t) = Gt^l \cosh rt, \quad r, l \in N.$ Using the procedure discussed in section 3, we can convert the given message $G_{i,0}$ to $G_{i,1}$,

where

$$q_{i,1} = (G_{i,0} r^{2i} (2i+1)(2i+2)\cdots(2i+l) + p),$$
$$i, l = 0,1,2,\cdots, \qquad (3.14)$$

with key

$$k_{i,1} = \frac{q_{i,1} - G_{i,1}}{26}, \; i = 0,1,2,3,\cdots. \qquad (3.15)$$

Hence we have following generalized theorem

Theorem 3.4: The given plain text in terms of $G_{i,0}, \; i = 1,2,3,\cdots,$ *under Laplace transform of* $G_{i,0} t^l \cosh rt,$ *(that is by writing them as a coefficients of* $t^l \cosh rt,$ *and then taking the Laplace transform) can be converted to cipher text*

$$G_{i,1} = (G_{i.0}\, r^{2i} (2i+1)(2i+2)\cdots$$
$$(2i+l) \; + p) \bmod 26$$
$$= q_{i,1} - 26k_{i,1}, \; i, l = 0,1,2,3,\cdots, \qquad (3.16)$$

with $q_{i,1}$ *and* $k_{i,1}$ *are given by* (3.14) *and* (3.15) *respectively.*

Remark 4.1: Theorem 3.3 is a special case of theorem 3.4 with $l = 2, r = 2.$

Now we apply above operations successively j times on the output obtained in the last step on the cipher text and obtain new cipher text this is included in the following new theorem.

Theorem 3.5: The given plain text in terms of $G_{i,0}, \; i = 1,2,3,\cdots,$ *under Laplace transform of* $G_{i,0} t^l \cosh rt,$ *successively j times (that is by writing them as a coefficients of* $t^l \cosh rt,$ *and then taking the Laplace transform successively) can be converted to cipher text*

$$G_{i,j} = (G_{i,j-1}\; r^{2i} (2i+1)(2i+2)\cdots(2i+l) + p) \bmod 26$$
$$= q_{i,j} - 26k_{i,j}, \; i, j, l = 0,1,2,3,\cdots, \qquad (3.17)$$

and

$$q_{i,j} = (G_{i,j-1} r^{2i} (2i+1)(2i+2)\cdots(2i+l) + p), \; i, j, l = 0,1,2,3,\cdots, \qquad (3.18)$$

and key

$$k_{i,j} = \frac{q_{i,j} - G_{i,j}}{26}, \;\; i, j = 0,1,2,3,\cdots,. \qquad (3.19)$$

Remark 3.2: Theorem 3.4 is a special case of Theorem 3.5 with $j = 1.$ Hence all Theorems 3.1 to 3.4 follows from Theorem 3.5.

IV. DECRYPTION

For the decryption of the received cipher text we proceed exactly in the reverse direction using inverse Laplace transform. The method is as follows.

Suppose we have received message as 'UUQEIG' which is equivalent to

20 20 16 4 8 6.

Let us assume that

$G_{0,1}$ = 20, $G_{1,1}$ = 20, $G_{2,1}$ = 16, $G_{3,1}$ = 4, $G_{4,1}$ = 8 $G_{5,1}$ = 6, $G_{n,1}$ = 0 for n ≥ 6.

Using given key $k_{i,0}, \; i = 0,1,2,3,\cdots$ as

0 31 369 1103 16837 93578

and $p = 10,$ assuming

$$q_{i,1} = G_{i,1} + 26k_{i,1} - p, \; i = 0,1,2,3,\cdots.. \qquad (4.1)$$

We consider

$$G\left(-\frac{d}{ds}\right)^2 \frac{s}{\left(s^2 - 2^2\right)}$$
$$= \frac{10}{s^3} + \frac{816}{s^5} + \frac{9600}{s^7} + \frac{28672}{s^9} + \frac{437760}{s^{11}} + \frac{2433024}{s^{13}}$$
$$= \sum_{i=0}^{n} \frac{q_{i,1}}{s^{2i+3}}. \qquad (4.2)$$

Taking inverse Laplace transform we get

$$f(t) = Gt^2 \cosh 2t$$
$$= \sum_{i=0}^{\infty} \frac{2^{2i} t^{2i+2} G_{i,0}}{2i!}$$
$$= 5\frac{t^2}{0!} + 17\frac{2^2 t^4}{2!} + 20\frac{2^4 t^6}{4!} + 8\frac{2^6 t^8}{6!} + 19\frac{2^8 t^{10}}{8!} + 18\frac{2^{10} t^{12}}{10!}.$$

$$= t^2[G_{0,0} + G_{1,0}\frac{2^2 t^2}{2!} + G_{2,0}\frac{2^4 t^4}{4!} + G_{3,0}\frac{2^6 t^6}{6!} \qquad (4.3)$$
$$+ G_{4,0}\frac{2^8 t^8}{8!} + G_{5,0}\frac{2^{10} t^{10}}{10!}]$$

Here we have

$G_{0,0} = 5$, $G_{1,0} = 17$, $G_{2,0} = 20$, $G_{3,0} = 8$, $G_{4,0} = 19$, $G_{5,0} = 18$, $G_{n,0} = 0$ for n ≥ 6.

Here message
$5 \quad 17 \quad 20 \quad 8 \quad 19 \quad 18.$ is equivalent to 'FRUITS'. Thus 'UUQEIG' under inverse Laplace transform gets converted to 'FRUITS'. Hence we have following decryption theorem

Theorem 4.1: The given cipher text in terms of $G_{i,1},\ i=1,2,3,\cdots,$ *with a given key* $k_{i,0},\ i=0,1,2,3,\cdots$ *can be converted to plain text* $G_{i,0}$ *under the inverse Laplace transform of*

$$G\left(-\frac{d}{ds}\right)^2 \frac{s}{\left(s^2-2^2\right)}=\sum_{i=0}^{n}\frac{q_{i,0}}{s^{2i+3}}, \qquad (4.4)$$

where

$$G_{i,0}=\frac{26k_{i,0}+G_{i,1}-p}{2^{2i}\left(2i+1\right)\left(2i+2\right)},\ i=0,1,2,3,\cdots,p\in N, \quad 0\le p\le 25, \qquad (4.5)$$

and $q_{i,0}=26k_{i,0}+G_{i,1},\ i=0,1,2,3,\cdots.$ (4.6)

The generalized iterative theorem can be obtained on the similar way which is included in the following

Theorem 4.2: The given cipher text in terms of $G_{i,j},\ i,j=1,2,3\cdots,$ *with a given key* $k_{i,j-1},\ i,j=1,2,3\cdots,$ *can be converted to plain text* $G_{i,j-1}$ *under the inverse Laplace transform of*

$$G\left(-\frac{d}{ds}\right)^2 \frac{s}{\left(s^2-2^2\right)}=\sum_{i=0}^{n}\frac{q_{i,j-1}}{s^{2i+3}}, \qquad (4.7)$$

where

$$G_{i,j-1}=\frac{26k_{i,j-1}+G_{i,j}-p}{2^{2i}\left(2i+1\right)\left(2i+2\right)},\ i,j=1,2,3,\cdots,p\in N, \quad 0\le p\le 25, \qquad (4.8)$$

and $q_{i,j}=26k_{i,j}+G_{i,j},\ i,j=1,2,3,\cdots,$ (4.9)

Remark 4.1: Results in [6], G.Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar are obtained by considering Laplace transform te^t and are generalized in Hiwarekar A.P. [8], [9].

The method developed in this paper can be used in the form of following algorithm.

V. ENCRYPTION ALGORITHM

1) Treat every letter in the plain text message as a number so that $A=0;B=1;C=2;\cdots,Z=25.$

2) The plain text message $G_{i,0}$ is organized as a finite sequence of numbers, based on the above conversion. Only consider $G_{i,0}$ till the length of input string, i.e. $i=1$ to $n-1.$

3) Consider suitable function $f(t)$ as in Theorem 3.5, choose suitable values of $l,r,j,p.$ Take successive Laplace transform of $f(t)$ and get formula (3.17) for encryption. Hence each character in the input string converts to new position $G_{i,\mathrm{j}}.$

4) Key values $K_{i,\mathrm{j}}$ for every character can be obtained by equation (3.19) using (3.18).

5) Send $G_{i,\mathrm{j}-1}$ and $K_{i,\mathrm{j}}$ as well as l,r,j,p to the receiver.

On similar way we can also obtain decryption algorithm.

5.1. Illustrative Examples

Using results obtained in Theorem 3.3, if we have original message 'FRUITS', then it gets converted to

1. 'WCUMUW' for $l=2,r=3,j=4,p=10,$
2. 'LRNVLV' for $l=2,r=2,j=3,p=7,$
3. 'GQCIIG' for $l=3,r=4,j=5,p=6,$
4. 'WUYIME' for $l=3,r=5,j=6,p=4,$
5. 'AUOKKE' for $l=3,r=5,j=2,p=4.$

5.2 Implementation Strategies

The main advantage of this algorithm is for same input alphabets we can get different output alphabets. We just need to change values of l or r or j or p or all of them (in theorem 3.3). Algorithm may prevent different attacks on the symmetric encryption such as cipher text only, known plaintext, chosen plaintext, chosen cipher text, chosen text. Moreover we can divide the document into blocks of four to six alphabets. Apply Encryption on these blocks in parallel and generate cipher text as well as the keys respectively. If we consider encryption of one complete document then we can choose different values of 'r' (in Theorem 3.5) for different blocks. For each block chose different value of r so that by any way attacker cracked one block he will not be able to crack other blocks. We can also apply iterative method in some cases. This will resist all types of attacks mentioned earlier. For Brute Force attack large amount of calculations will be needed as attacker doesn't know the algorithm as well as we are adding extra layer of security by using variable values of l or r or j or p or all of them at a time (in Theorem 3.5). Other aspect of algorithm is key length it can be considered as advantage in some applications or disadvantage in case of data length limited applications.

VI. DISCUSSION AND CONCLUDING REMARKS

1. 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. The new method of key generation scheme developed in this paper may be used for a fraud prevention mechanism.
2. In the proposed work we develop a new cryptographic scheme using Laplace transforms and the key is the number of multiples of mod n. Therefore it is very difficult for an eyedropper to trace the key by any attack. The results in section 3 provide as many transformations as per the requirements which is the most useful factor for changing key.
3. The similar results can be obtained by using Laplace transform of other suitable function. Hence extension of this work is possible. Moreover the entire document can be encrypted by considering block ciphers of small sizes.
4. For computer network security random number generation is a prime important task and also it is very essential in constructing keys for cryptographic algorithm. Method used in this paper can be useful for random number generation.
5. To reduce the crypt-analysis attack risk, a dynamic key theory plays important role, the method presented in this paper is useful in such situations.

ACKNOWLEDGEMENTS

Author is thankful to Principal Dr. S. B. Deosarkar and Vidya Pratishthan's College of Engineering, Baramati, Dist. Pune, Maharashtra, India, for the support to this work.

REFERENCES

[1] Alexander Stanoyevitch, Introduction to cyrptography 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 1999, Proceedings of the IEEE Symposium, 9-12, (May1999).

[4] Eric C., Ronald K., James W.C., Netwark SecurityBible Second edn.,Wiley India pub.(2009).

[5] Erwin Kreyszing, Advanced Engineering Mathematics, John Wiley and Sons Inc.(1999).

[6] 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).

[7] Grewal B.S., Higher Engineering Mathematics, Khanna Pub., Delhi, (2005).

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

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

[10] Hiwarekar A.P., Application of Laplace Transform for Cryptographic Scheme, proceeding of World Congress on Engineering Vol.II, LNCS, 95-100, (2013).

[11] Hiwarekar A.P., New Mathematical Modeling for Cryptography, Journal of Information Assurance and Security, MIR Lab USA, Vol. 9, 027-033, (2014).

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

[13] Lokenath Debnath, Dambaru Bhatta, Integrl Transforms and Their Applications, Chapman and Hall/CRC, First Indian edn. (2010).

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

[15] Ramana B.V., Higher Engineering Mathematics, Tata McGraw-Hills, (2007).

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

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

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