International Journal of Mathematical Archive-4(2), 2013, 208-213
IJMA Available online through www.ijma.info ISSN 2229 – 5046

A NEW METHOD OF CRYPTOGRAPHY USING LAPLACE TRANSFORM OF HYPERBOLIC FUNCTIONS

A. P. Hiwarekar*
Vidya Pratishthan's College of Engineering, Vidyanagari, M. I. D. C. Baramati,
Dist.Pune, Maharashtra, India, Pin-413133

(Received on: 13-01-13; Revised & Accepted on: 19-02-13)

ABSTRACT

Network security is very important in the Internet and other form of electronic communications such as mobile communications, Pay-TV, e- commerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords, etc, which touches on many aspects of our daily lives.

In this paper we developed a new algorithm for cryptography, in which we used Laplace transform of hyperbolic functions for encrypting the plain text and corresponding inverse Laplace transform for decryption. Starting with basic theory of Laplace transforms in section 2, we obtained the main results in section 3. The generalization of the results are included in section 4. This paper is based on the work of [5], A. P. Hiwarekar and [6], G. Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar.

Key words: *Cryptography, Data encryption, Applications to coding theory and cryptography, Algebraic coding theory; cryptography, Laplace transforms.*

Mathematics Subject classification: *94A60, 68P25, 14G50, 11T71, 44A10.*

1. INTRODUCTION

The fundamental objective of cryptography is to enable two people, to communicate over an insecure channel in such a way that an opponent cannot understand what is being said. Encryption is the process of obscuring information to make it unreadable without special knowledge. This is usually done for secrecy and typically for confidential communications. A cipher is an algorithm for performing encryption (and the reverse, decryption) a series of well-defined steps that can be followed as a procedure. The original information is known as plain text, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it. Ciphers are usually parameterized by a piece of auxiliary information, called a key. The encrypting procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt, or more importantly, to decrypt, [1, 2, 3, 5, 6, 7, 9, 10, 11].

2. DEFINITIONS AND STANDARD RESULTS

Laplace transform has many applications in various fields such as Mechanics, Electrical circuit, Beam problems, Heat conduction, Wave equation, Transmission lines, Signals and systems, Control systems, Communication systems, Hydrodynamics, Solar systems, [4,8]. In this paper we discuss its application to cryptography.

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

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

provided that the integral exists. Here the parameter s is a real or complex number. The corresponding inverse Laplace transform is $L^{-1}\{F(s)\} = f(t)$. Here $f(t)$ and $F(s)$ are called as pair of Laplace transforms, [4, 8].

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

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

then $$L\{c_1 f_1(t) + c_2 f_2(t) + \cdots c_n f_n(t)\} = c_1F_1(s) + c_2F_2(s) + \cdots + c_nF_n(s), \tag{2.3}$$

Corresponding author: *A. P. Hiwarekar*, Vidya Pratishthan's College of Engineering, Vidyanagari, M. I. D. C. Baramati, Dist.Pune, Maharashtra, India, Pin-413133*

where $c_1, c_2, \cdots, c_n$ are constants, [4, 8].

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 consider following standard results of Laplace transform

$$1.\ L\{\sinh kt\} = \frac{k}{s^2 - k^2}, \qquad \text{and} \qquad L^{-1}\{\frac{k}{s^2 - k^2}\} = \sinh kt. \tag{2.4}$$

$$2.\ L\{t^n\} = \frac{n!}{s^{n+1}}, \quad n \in N, \qquad \text{and} \qquad L\{\frac{n!}{s^{n+1}}\} = t^n, \quad n \in N. \tag{2.5}$$

$$3.\ L\{t^n f(t)\} = \left(\frac{-d}{ds}\right)^n F(s), \qquad \text{and} \qquad L^{-1}\{\left(\frac{-d}{ds}\right)^n F(s)\} = t^n f(t), \quad [4, 8]. \tag{2.6}$$

3. MAIN RESULTS

3.1 Encryption

We consider standard expansion

$$\sinh rt = rt + \frac{r^3t^3}{3!} + \frac{r^5t^5}{5!} + \frac{r^7t^7}{7!} + \cdots + \frac{r^{2i+1}t^{2i+1}}{2i+1!} + \cdots + \cdots = \sum_{i=0}^{\infty} \frac{(rt)^{2i+1}}{2i+1!}, \tag{3.1}$$

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

$$t^2 \sinh 2t = 2t^3 + \frac{2^3t^5}{3!} + \frac{2^5t^7}{5!} + \frac{2^7t^9}{7!} + \cdots + \frac{2^{2i+1}t^{2i+3}}{2i+1!} + \cdots + \cdots = \sum_{i=0}^{\infty} \frac{2^{2i+1}t^{2i+3}}{2i+1!}. \tag{3.2}$$

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

Let given message called plaintext be 'SECURENET', it is equivalent to

18 4 2 20 17 4 13 4 19.

Let us assume that

$G_0 = 18, \quad G_1 = 4, \quad G_2 = 2, \quad G_3 = 20, \quad G_4 = 17, \quad G_5 = 13, \quad G_6 = 4,$

$G_7 = 19, \quad G_n = 0 \quad \text{for n} \geq 9.$

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

$$\begin{aligned} f(t) &= t^2[G_0.2t + G_1\frac{2^3t^3}{3!} + G_2\frac{2^5t^5}{5!} + G_3\frac{2^7t^7}{7!} + G_4\frac{2^9t^9}{9!} + G_5\frac{2^{11}t^{11}}{11!} + G_6\frac{2^{13}t^{13}}{13!} + G_7\frac{2^{15}t^{15}}{15!} + G_8\frac{2^{17}t^{17}}{17!}] \\ &= \sum_{i=0}^{\infty} \frac{2^{2i+1}t^{2i+3}G_i}{2i+1!} \\ &= 18\frac{2t^3}{1!} + 4\frac{2^3t^5}{3!} + 2\frac{2^5t^7}{5!} + 20\frac{2^7t^9}{7!} + 17\frac{2^9t^{11}}{9!} + 4\frac{2^{11}t^{13}}{11!} + 13\frac{2^{13}t^{15}}{13!} + 4\frac{2^{15}t^{17}}{15!} + 19\frac{2^{17}t^{19}}{17!}. \end{aligned} \tag{3.3}$$

Taking Laplace transform on both sides we have

$$\begin{aligned} L\{f(t)\} &= L\{Gt^2 \sinh 2t\} \\ &= \frac{216}{s^4} + \frac{640}{s^6} + \frac{2688}{s^8} + \frac{184320}{s^{10}} + \frac{957440}{s^{12}} + \frac{1277952}{s^{14}} + \frac{22364160}{s^{16}} + \frac{35651584}{s^{18}} + \frac{851705856}{s^{20}}. \end{aligned} \tag{3.4}$$

Adjusting the resultant values

216 640 2688 184320 957440 1277952 22364160 35651584 851705856 to mod 26, that is

$216 = 8 \bmod 26, \qquad 640 = 16 \bmod 26, \qquad 2688 = 10 \bmod 26,$

$184320 = 6 \bmod 26, \qquad 957440 = 16 \bmod 26, \qquad 1277952 = 0 \bmod 26,$

$22364160 = 0 \bmod 26, \qquad 35651585 = 20 \bmod 26, \qquad 851705856 = 14 \bmod 26.$

Sender sends the values 8 24 103 7089 36824 49152 860160 1371214 32757917 as a key.

Assuming $G'_0 = 8,\quad G'_1 = 16,\quad G'_2 = 10,\quad G'_3 = 6,\quad G'_4 = 16,\quad G'_5 = 0,$
$G'_6 = 0,\quad G'_7 = 20,\quad G'_8 = 14,\quad G'_n = 0$ for n ≥ 9.

The given plain text gets converted to cipher text
8 16 10 6 16 0 0 20 14.

Here message 'SECURENET' gets converted to 'IQKGQAAUO'.

Hence we have following

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

$$G'_i = q_i - 26k_i, \quad for\ i = 0,1,2,3,\cdots, \tag{3.5}$$

where,

$$q_i = 2^{2i+1}\left(2i+3\right)\left(2i+2\right)G_i \qquad for\ i = 0,1,2,3,\cdots, \tag{3.6}$$

and a key

$$k_i = \frac{q_i - G'_i}{26} \quad for\ i = 0,1,2,3,\cdots. \tag{3.7}$$

3.2 Decryption

We have received message as 'IQKGQAAUO' which is equivalent to 8 16 10 6 16 0 0 20 14.

Let us assume that

$G'_0 = 8,\quad G'_1 = 16,\quad G'_2 = 10,\quad G'_3 = 6,\quad G'_4 = 16,\quad G'_5 = 0,$
$G'_6 = 0,\quad G'_7 = 20,\quad G'_8 = 14,\quad G'_n = 0$ for n ≥ 9.

Using given key $k_i\ for\ i = 0,1,2,3,\cdots$ as
8 24 103 7089 36824 49152 860160 1371214 32757917

and assuming

$$q_i = 26k_i + G'_i \quad for\ i = 0,1,2,3,\cdots. \tag{3.8}$$

We consider

$$G\left(-\frac{d}{ds}\right)^2 \frac{2}{\left(s^2-2^2\right)} = \frac{216}{s^4} + \frac{640}{s^6} + \frac{2688}{s^8} + \frac{184320}{s^{10}} + \frac{957440}{s^{12}} + \frac{1277952}{s^{14}} + \frac{22364160}{s^{16}} + \frac{35651584}{s^{18}} + \frac{851705856}{s^{20}}. \tag{3.9}$$

$$= \sum_{i=0}^{n} \frac{q_i}{s^{2i+4}}.$$

Taking inverse Laplace transform we get

$$f(t) = Gt^2 \sinh 2t$$

$$= 18\frac{2t^3}{1!} + 4\frac{2^3t^5}{3!} + 2\frac{2^5t^7}{5!} + 20\frac{2^7t^9}{7!} + 17\frac{2^9t^{11}}{9!} + 4\frac{2^{11}t^{13}}{11!} + 13\frac{2^{13}t^{15}}{13!} + 4\frac{2^{15}t^{17}}{15!} + 19\frac{2^{17}t^{19}}{17!}. \tag{3.10}$$

Here we have

$G_0 = 18,\quad G_1 = 4,\quad G_2 = 2,\quad G_3 = 20,\quad G_4 = 17,\quad G_5 = 4,\quad G_6 = 13,$
$G_7 = 4,\quad G_8 = 19,\quad G_n = 0$ for n ≥ 9.

Here 18 4 2 20 17 4 13 4 19, is equivalent to 'SECURENET'.

Hence we have following

Theorem 3.2: *The given cipher text in terms of* $G'_i,\ i=1,2,3,\cdots,$ *with a given key* k_i *for* $i=0,1,2,3,\cdots,$ *can be converted to plain text* G_i *under the inverse Laplace transform of*

$$G\left(-\frac{d}{ds}\right)^2\frac{2}{\left(s^2-2^2\right)}=\sum_{i=0}^{n}\frac{q_i}{s^{2i+4}}, \tag{3.11}$$

where $$G_i=\frac{26k_i+G'_i}{2^{2i+1}\left(2i+2\right)\left(2i+3\right)}\quad for\ i=0,1,2,3,\cdots, \tag{3.12}$$

and $$q_i=26k_i+G'_i,\quad for\ i=0,1,2,3,\cdots. \tag{3.13}$$

4. GENERALIZATION

4.1. Case-1: For encryption of given message in terms of G_i, we consider

$$t^2\sinh rt=rt^3+\frac{r^3t^5}{3!}+\frac{r^5t^7}{5!}+\frac{r^7t^9}{7!}+\cdots+\frac{r^{2i+1}t^{2i+3}}{2i+1!}+\cdots+\cdots=\sum_{i=0}^{\infty}\frac{r^{2i+1}t^{2i+3}}{2i+1!}, \tag{4.1}$$

and $f(t)=Gt^2\sinh rt,\ r\in N.$ Taking Laplace transform and using the procedure discussed in section 3, then we can convert the given message G_i to G'_i where

$$q_i=G_ir^{2i+1}\left(2i+3\right)\left(2i+2\right),\ i=0,1,2,\cdots, \tag{4.2}$$

where

$$q_i=G_ir^{2i+1}\left(2i+3\right)\left(2i+2\right)\quad i=0,1,2,\cdots, \tag{4.3}$$

with key $k_i=\dfrac{q_i-G'_i}{26}\quad for\ i=0,1,2,3,\cdots.$ (4.4)

Hence we have following

Theorem 4.1: *The given plain text in terms of* $G_i,\ i=1,2,3,\cdots,$ *under Laplace transform of* $Gt^2\sinh rt,\ r\in N,$ *(that is by writing them as a coefficients of* $t^2\sinh rt,$ *and then taking the Laplace transform) can be converted to cipher text* $G'_i,\ i=1,2,3,\cdots,$
where,

$$G'_i=q_i-26k_i,\quad for\ i=0,1,2,3,\cdots, \tag{4.5}$$

with q_i *and* k_i *are given by* (4.3) *and* (4.4) *respectively.*

For decryption of received message in terms of G'_i we consider

$$G\left(-\frac{d}{ds}\right)^2\frac{r}{\left(s^2-r^2\right)}\ =\ \sum_{i=0}^{\infty}\frac{q_i}{s^{2i+4}}. \tag{4.6}$$

Taking inverse Laplace transform and using procedure discussed in section 3, we can convert given message G'_i to G_i. Hence we have following

Theorem 4.2: *The given cipher text in terms of* $G'_i,\ i=1,2,3,\cdots,$ *with given key* k_i *for* $i=0,1,2,3,\cdots,$ *under the inverse Laplace transform of*

$$G\left(-\frac{d}{ds}\right)^2\frac{r}{\left(s^2-r^2\right)}=\sum_{i=0}^{n}\frac{q_i}{s^{2i+4}},\quad for\ r\in N,$$

can be converted to plain text G_i, $i = 1, 2, 3, \cdots$, *given by*

$$G_i = \frac{26k_i + G'_i}{r^{2i+1}(2i+2)(2i+3)}, \ r \in N, \ i = 0,1,2\cdots. \tag{4.7}$$

where $$q_i = 26k_i + G'_i, \quad for \ i = 0,1,2,3,\cdots. \tag{4.8}$$

4.2 Case-2: For encryption of given message in terms of G_i we consider $f(t) = Gt^j \sinh rt, \ \ r, j \in N.$ Taking Laplace transform and we follow the procedure discussed in section 3,then we can convert the given message G_i to G'_i.
where

$$q_i = G_i r^{2i+1}(2i+2)(2i+3)\cdots(2i+j+1), \qquad i = 0,1,2,\cdots, \tag{4.9}$$

with private key $k_i = \dfrac{q_i - G'_i}{26}$ $\quad for \ i = 0,1,2,3,\cdots.$ (4.10)

Hence we have

Theorem 4.3: *The given plain text in terms of* G_i, $i = 1, 2, 3, \cdots,$ *under Laplace transform of* $Gt^j \sinh rt, \ r, j \in N$ *(that is by writing them as a coefficients of* $t^j \sinh rt$, *and then taking the Laplace transform) can be converted to cipher text*

$$G_i' = G_i r^{2i+1}(2i+2)(2i+3)\cdots(2i+j+1) \mod 26 = q_i \mod 26, \tag{4.11}$$

with q_i *and* k_i *are given by* (4.9) *and* (4.10) *respectively.*

For decryption of received message in terms of G'_i, we consider

$$G\left(\frac{-d}{ds}\right)^j \frac{r}{\left(s^2 - r^2\right)^{j+1}} = \sum_{i=0}^{\infty} \frac{q_i}{s^{2i+2+j}}. \tag{4.12}$$

Taking inverse Laplace transform and using procedure discussed in section 3, we can convert given massage G'_i to G_i where

$$G_i = \frac{26k_i + G'_i}{r^{2i+1}(2i+2)(2i+3)\cdots(2i+j+1)}, \quad i = 0,1,2\cdots. \tag{4.13}$$

Theorem 4.4: *The given cipher text in terms of* G'_i, $i = 1, 2, 3, \cdots,$ *with given key* $k_i \ for \ i = 0,1,2,3,\cdots,$ *Under the inverse Laplace transform of*

$$G\left(\frac{-d}{ds}\right)^j \frac{r}{\left(s^2 - r^2\right)^{j+1}} = \sum_{i=0}^{\infty} \frac{q_i}{s^{2i+2+j}}, \ r, j \in N, \tag{4.14}$$

can be converted to plain text G_i, $i = 1, 2, 3, \cdots,$ *given by* (4.13)
where

$$q_i = 26k_i + G'_i, \quad for \ i = 0,1,2,3,\cdots. \tag{4.15}$$

Remark 4.1: Results in [6], G.Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar are obtained by considering Laplace transform te^t on similar way as discussed in section 3 of this paper and are generalized in [5], A. P. Hiwarekar. Results in [3], G.A. Dhanorkar and A. P. Hiwarekar are obtained by using generalized Hill cipher algorithms.

4.1. Illustrative Examples

Using results obtained in this paper, if we have original message 'SECURENET', then it gets converted to

1. 'EQEMOQAMK' for $r = 3, j = 1,$
2. 'ECGKYAAWY' for $r = 1, j = 2,$

3. ‘QMWWCAAGM’ for $r=1, j=3,$
4. ‘GSCIKAAWU’ for $r=2, j=3,$
5. ‘CSGUKAAWA’ for $r=5, j=3.$

DISCUSSION AND CONCLUDING REMARKS

1. For the breaking a key of 256 bit by Bruce force attack, when faster super computer are used, it requires about 3:31×10^{56} years, which is almost impossible. Here for faster super computer,(as per wikipedia) 10:51 pentaops = 10:51×10^{15} flops.

2. 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 (e-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.

3. 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 4 provide as many transformations as per the requirements which is the most useful factor for changing key.

4. The similar results can be obtained by using Laplace transform of hyperbolic cosine functions as well as trigonometric sine and cosine functions. Hence extension of this work is possible.

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. Author is also thankful to BCUD University of Pune, India, for the financial support to this work under research project `Better network security using generalised Hill cipher algoritham'.

REFERENCES

[1] T.H.Barr, Invitation to Cryptography, Prentice Hall, 2002.

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

[3] G.A. Dhanorkar and A.P.Hiwarekar, A generalized Hill cipher using matrix transformation, International J. of Math. Sci. & Engg. Appls. Vol. 5, No. IV (July, 2011), pp 19-23.

[4] B. S. Grewal, Higher Engineering Mathematics, Khanna Pub. Delhi, 2005.

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

[6] G.Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar, A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2(12) (2011), pp 2515-2519.

[7] J. Overbey, W. Traves and J. Wojdylo, On the Keyspace of the Hill Cipher, Cryptologia, 29(1) (January 2005), pp 59-72.

[8] B. V. Ramana, Higher Engineering Mathematics, Tata McGraw-Hills, 2007.

[9] S.Saeednia, How to Make the Hill Cipher Secure, Cryptologia, 24(4) (October 2000), pp 353-360.

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

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

Source of support: Nil, Conflict of interest: None Declared