PSYCHOLOGY AND EDUCATION (2021) 58(5), ISSN 1553 - 6939
Article Received: 22th November, 2020; Article Revised: 26th March, 2021; Article Accepted: 26th April, 2021

New Method for Cryptography using Laplace-Elzaki Transform

JadhavShailaShivaji[1], Hiwarekar A.P.[2]
[1] Ph. D. Scholar, Shri. JJT University, Vidyanagari, Rajasthan, India
[2] Vidya Pratishthans Kamalnayan Bajaj Institute of Engineering and Technology,Baramati, Baramati, India
[1] shailajadhavbhosale@gmail.com, [2] hiwarekaranil@gmail.com

ABSTRACT

Cryptography is very useful in a communication system for authentication and privacy. It affects many activities in our life. In this paper, we developed a new technique for cryptography using Elzaki and Laplace transforms. Further, we apply the method of iteration for better security. On the other hand, we apply inverse Laplace transform and then inverse Elzaki transform for decryption. Due to the use of iterations, the level of security increases, and the method is more applicable

Keywords

Laplace transform, Elzaki transform, Encryption, Decryption.

Introduction

In the world most of the peoples use the internet for the transaction, sharing useful information using e-mail, online payment, business, video conferencing, online shopping, etc. and for all such activities, security is essential. For this security purpose, cryptography is useful. Cryptography is useful to hide private information such as documents, ATM passwords, transaction passwords, etc. and communicate in such a way that the only recipient understands the message. Various methods of cryptography are found in the literature. G. Naga Lakshmi, [3] gave the method of cryptography by using Laplace transform, Hiwarekar A. P., [5], [6], [7] developed various methods for encryption and decryption using series expansion and it's Laplace transform, MampiSaha, [10] gave the method of cryptography using Laplace-Mellin transform, Chitra P. L., [12] defined method of encryption using wedges algorithm, etc.

Definitions And Standardresults

A. Exponential order

A function $F(t)$ is said to be of Exponential order α, as $t \to \infty$ if there exist positive constants M and K such that $|F(t)| \le Ke^{\alpha t}$, for all $t > M$.

B. Piecewise Continuous Function

A function $F(t)$ is said to be piecewise continuous on the interval $I = [c, d]$ if it is defined and continuous on interval I except a finite number of points, $t_1, t_2, \ldots, t_m$ at each of which the left and right limits of this function exist.

C. Laplace Transform

If $\mathrm{F}(t)$ is function of $t \ge 0$ then, Laplace transform of $F(t)$ is defined as,

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

Provided integral in (1) exists.Where L is a Laplace transform operator.

If the function $F(t)$ is piecewise continuous on $[0, \infty)$ and of exponential order α then Laplace transform exists for $\mathrm{Re}(s) > \alpha$. Also,

a) $$L(t^n) = \frac{n!}{s^{n+1}}, n \in \mathrm{N}, n \in N. \qquad (2)$$

D. Linearity Property of Laplace transform

Let $F(t)$ and $G(t)$ are two functions of $t > 0$, a, b are arbitrary constants then,

$$L\{aF(t) + bG(t)\} = aL\{F(t)\} + bL\{G(t)\}. \qquad (3)$$

E. Inverse Laplace Transform

If $L\{F(t)\} = f(s)$ then inverse Laplace transform of $f(s)$ is $\mathrm{F}(t)$, denoted by

$$L^{-1}\{f(s)\} = F(t). \qquad (4)$$

F. Linearity property of inverse Laplace transforms

If $L\{F(t)\} = f(s)$ and $L\{G(t)\} = \mathrm{g}(s)$ then

$$\mathrm{L}^{-1}\{f(s) + g(s)\} = \mathrm{L}^{-1}\{f(s)\} + \mathrm{L}^{-1}\{g(s)\}. \qquad (5)$$

G. Elzaki transform

The Elzaki transform of function $F(t)$ is defined as,

$$E\{F(t)\}=v\int_0^\infty F(t)e^{\frac{-t}{v}}dt,\ t\geq 0,\ k_1\leq v\leq k_2, \quad (6)$$

provided that integral in (6) exists. Where E isElzaki transform operator.

If function $F(t),\ t\geq 0$ is piecewise continuous and of exponential order then Elzaki transform of function $F(t)$ exist.

H. Inverse Elzaki transform

If $E\{F(t)\}=T(v)$,then inverse Elzaki transform of $T(v)$ is $F(t)$ denoted it by

$$E^{-1}\{T(v)\}=F(t). \quad (7)$$

Also,

$$E(t^n)= n!\ v^{n+2},\ n\in N. \quad (8)$$

I. Cipher Text

It is conversion of plain text by using suitable method of cryptography.

J. Encryption method

The method in which plain text converted into cipher text by suitable technique called as encryption method.

K. Decryption method

The method in which cipher text converted into plain text by suitable technique called as decryption method.

Cryptographic Technique

A. Encryption

Consider the function

$$\mathrm{F}(t)= f_n^{\,j}te^t=\sum_{n=0}^{\infty} f_n^{\,j}\frac{t^{n+1}}{n!}, \quad (9)$$

and let plain text be 'TIME'.To encrypt plain text 'TIME' we convert alphabets to numbers by allocating,

$$A=0,\quad B=1,\ C=2,\quad D=3,\ E=4,$$
$$F=5,\quad G=6,\ H=7,\ I=8,\ J=9,$$
$$K=10,\ L=11, M=12,\ N=13,\ O=14,$$
$$P=15,\ Q=16,\ R=17,\ S=18,\ T=19,$$
$$U=20,\ V=21, W=22,\ X=23, Y=24,$$
$$Z=25.$$

a. First iteration

For first iteration $j=0$,let

$\mathrm{T}= f_0^{\,0}=19,\ \mathrm{I}= f_1^{\,0}=8,\ \mathrm{M}= f_2^{\,0}=12,\ \mathrm{E}= f_3^{\,0}=4$ and $f_n^{\,0}=0$ for $n\geq 4$ and treating these number's as coefficients of te^t and $\mathrm{F}(t)= f_n^{\circ}te^t$ by iterative method.

$$F(t)= f_0^{\,0}t+ f_1^{\,0}t^2+ f_2^{\,0}\frac{t^3}{2!}+ f_3^{\,0}\frac{t^4}{3!}$$
$$=19t+8t^2+12\frac{t^3}{2!}+4\frac{t^4}{3!}. \quad (10)$$

Taking Elzaki transform of $F(t)$ on both sides,

$$E(F(t))=19u^3+8\times(2!)u^4+\frac{12}{2!}\times(3!)u^5+\frac{4}{3!}\times(4!)u^6. \quad (11)$$

Now $u>0$, taking Laplace transform of $E\{F(t)\}$,

$$L\left(\frac{f_n^{\,0}u^3}{(1-u)^2}\right)$$
$$=19\times\frac{3!}{s^4}+8\times(2!)\times\frac{4!}{s^5}+\frac{12}{2!}\times(3!)\times\frac{5!}{s^6}+\frac{4}{3!}\times(4!)\times\frac{6!}{s^7}$$
$$=\sum_{n=0}^{\infty}\frac{p_n^1}{s^{n+4}},\ p_n^1=0\ \forall n\geq 4. \quad (12)$$

We get, p_n^1 : 114 384 4320 11520, r_n^1: 4 14 166 443

where $f_n^1\equiv p_n^1(\mathrm{mod}\ 26),\ r_n^1=\dfrac{p_n^1-f_n^1}{26}$

$$f_n^1:\ 10\ \ 20\ \ 4\ \ 2. \quad (13)$$

Now in first iteration plain text 'TIME' becomes 'KUEC', repeat the same procedure for f_n^1.

b. Second iteration

If f_n^1 are given then consider,

PSYCHOLOGY AND EDUCATION (2021) 58(5), ISSN 1553 - 6939
Article Received: 22th November, 2020; Article Revised: 26th March, 2021; Article Accepted: 26th April, 2021

$$\mathrm{F}(t) = f_n^1 te^t$$
$$= f_0^1 t + f_1^1 t^2 + f_2^1 \frac{t^3}{2!} + f_3^1 \frac{t^4}{3!}$$
$$= 10\mathrm{t}+20\mathrm{t}^2 + 4\frac{t^3}{2!} + 2\frac{t^4}{3!}. \quad (14)$$

Taking Elzaki transform of both sides of (14) ,

$$\mathrm{E}\left(f_n^1 te^t \right)$$
$$= 10u^3 + 20\times(2!)u^4 + \frac{4}{2!}\times(3!)u^5 + \frac{2}{3!}\times(4!)u^6, \quad (15)$$

as $u > 0$ taking Laplace transform on both sides of (15) we get,

$$\mathrm{L}\left(f_n^1 \frac{u^3}{(1-u)^2} \right)$$
$$= 10\times\frac{3!}{s^4} + 20\times(2!)\times\frac{4!}{s^5} + 4\times\frac{3!}{2}\times\frac{5!}{s^6} + \frac{2}{3!}\times(4!)\times\frac{6!}{s^7}$$
$$= \sum_{n=0}^{\infty} \frac{p_n^2}{s^{n+4}},\ p_n^2 = 0 \text{ for } \mathrm{n} \geq 4, \quad (16)$$

$p_n^2 : 60\ \ 960\ \ 440\ \ 5760,$

$f_n^2 : 8\ \ 24\ \ 10\ \ 14,\ r_n^2 : 2\ 36\ 55\ 221$

and cipher text becomes ‘IYKO’.

c. Third Iteration

If f_n^2, r_n^2 are given then,

$$f_n^2 te^t = f_0^2 t + f_1^2 t^2 + f_2^2 \frac{t^3}{2!} + f_3^2 \frac{t^4}{3!}$$
$$= 8\mathrm{t}+24\mathrm{t}^2 + 10\frac{t^3}{2!} + 14\frac{t^4}{3!}. \quad (17)$$

Taking Elzaki transform of $f_n^2 te^t$

$$\mathrm{E}\left(f_n^2 te^t \right)$$
$$= 8u^3 + 24\times(2!)u^4 + \frac{10}{2!}\times(3!)u^5 + \frac{14}{3!}\times(4!)u^6. \quad (18)$$

Taking Laplace transform of $\left\{ E\left(f_n^2 te^t \right) \right\}$,

$$\mathrm{L}\left(\frac{f_n^2 u^3}{(1-u)^2} \right)$$
$$= 8\times\frac{3!}{s^4} + 24\times(2!)\times\frac{4!}{s^5} + \frac{10\times(3!)\times(5!)}{(2!)\times s^6} + \frac{14\times(4!)\times(6!)}{(3!)\times s^7}$$
$$= \frac{48}{s^4} + \frac{1152}{s^5} + \frac{3600}{s^6} + \frac{40320}{s^7}$$
$$= \sum_{n=0}^{\infty} \frac{p_n^3}{s^{n+4}},\ p_n^2 = 0\ \forall \mathrm{n} \geq 4, \quad (19)$$

Where,

$p_n^3 : 48\ \ 1152\ \ 3600\ \ 40320$, $f_n^3 \equiv p_n^3 \pmod{26}$,

$f_n^3 : 22\ \ 8\ \ 12\ \ 20$, $\mathrm{r}_n^3 : 1\ \ 44\ \ 138\ \ 1550.$

And cipher text is ‘WIMU’.

Here we apply three iterations to encrypt plain text ‘TIME’ we get cipher text ‘WIMU’.These results can be presented in the form of following theorems.

Theorem 3.1

The given plain text in terms of f_n^0, for $n = 0,1,2,......,$ under Elzaki transform of $f_n^0 te^t$ and then Laplace transform of $E[\, f_n^0 te^t\,]$ can be converted to cipher text coefficients,

$$f_n^1 = \left\{ (n+1)\left[(n+3)! \right] f_n^0 \right\} (\mathrm{mod}\ 26)$$
$$= p_n^1 \text{-} 26 r_n^1,\ n = 0,1,2,3........, \quad (20)$$

Where $p_n^1 = \left\{ (n+1)\left[(n+3)! \right] \right\} f_n^0$

For $n = 0,1,2,3......$ and

Key

$$r_n^1 = \frac{p_n^1 - f_n^1}{26},\ n = 0,1,2,........ \quad (21)$$

Byrepeating the same procedure on f_n^1, and we obtained f_n^2.

Similarly by Repeatingthe thisprocedure on f_n^2, we obtained f_n^3.

Its generalization is explained in the following:

Theorem 3.2

The given plain text in terms of f_n^0, $n = 0,1,2,.....,$ under Elzaki transform $f_n^0 te^t$ and then Laplace transform of $E[\, f_n^0 te^t\,]$ successively m times, can be converted into cipher text,

$$f_n^m = \{(n+1)[(n+3)!]\}^m f_n^0 (\text{mod } 26)$$
$$= p_n^m \text{-} 26r_n^m,\ n=0,1,2,....,\ m=1,2,3......, \quad (22)$$

where, $p_n^m = \{(n+1)[(n+3)!]\}^m f_n^0$ for $n=0,1,2,....,\ m=1,2,3,......$ and key

$$r_n^m = \frac{p_n^m - f_n^m}{26},\ n=0,1,2,......... . \quad (23)$$

B. Decryption

To obtained original text from encrypted message we apply reverse algorithm that is we proceed in the reverse direction which is included in the following

a. First iteration

If f_n^3 and r_n^3 are given as,
$f_n^3: 22\ \ 8\ \ 12\ \ 20,\ r_n^3: 1\ \ 44\ \ 138\ \ 1550,\ p_n^3 = 26r_n^3 + f_n^3.$

Then consider,

$$\left[-f_n^2\left(\frac{d^3}{ds^3}L\left(\frac{1}{(t-1)^2}\right)\right)\right] = \sum_{n=0}^{\infty}\frac{p_n^3}{s^{n+4}}$$
$$= \frac{48}{s^4}+\frac{1152}{s^5}+\frac{3600}{s^6}+\frac{40320}{s^7}. \quad (24)$$

Taking inverse Laplace transform of both sides of (24)

we get

$$\frac{f_n^2 u^3}{(1-u)^2} = 48\times\frac{u^3}{3!}+1152\times\frac{u^4}{4!}+3600\times\frac{u^5}{5!}+40320\times\frac{u^6}{6!}$$
$$= 8\text{u}^3+48\text{u}^4+30\text{u}^5+56\text{u}^6. \quad (25)$$

Taking inverse Elzaki transform of both sides of (25),

$$\text{E}^{-1}\left[\frac{f_n^2 u^3}{(1-u)^2}\right] = 8t+48\times\frac{t^2}{2!}+30\times\frac{t^3}{3!}+56\times\frac{t^4}{4!}$$
$$= \sum_{n=0}^{\infty} f_n^2\frac{t^{n+1}}{n!},\ f_n^2 = 0\ \forall n \geq 4. \quad (26)$$

Hence $f_n^2: 8\ \ 24\ \ 10\ \ 14$ and decoded message 'IYKO' is obtained in first iteration.

b. Second Iteration

If f_n^2 and r_n^2 are given, then apply the same procedure as above. Let,

$$[-f_n^1\{\frac{d^3}{ds^3}L(\frac{1}{(t-1)^2})\}] = \sum_{n=0}^{\infty}\frac{p_n^2}{s^{n+4}}$$
$$= \frac{60}{s^4}+\frac{960}{s^5}+\frac{1440}{s^6}+\frac{5760}{s^7}. \quad (27)$$

Taking inverse Laplace transform on both sides of (27)

$$f_n^1\frac{u^3}{(1-u)^2}$$
$$= 60\times\frac{u^3}{3!}+960\times\frac{u^4}{4!}+1440\times\frac{u^5}{5!}+5760\times\frac{u^6}{6!}$$
$$= 10\text{u}^3+40u^4+12u^5+8u^6. \quad (28)$$

Taking inverse Elzaki transform on both sides of (28)

$$E^{-1}\left[\frac{f_n^1 u^3}{(1-u)^2}\right] = 10\text{t}+40\times\frac{t^2}{2!}+12\times\frac{t^3}{3!}+8\times\frac{t^4}{4!}$$
$$= 10\text{t}+20\times\text{t}^2+4\times\frac{t^3}{2!}+2\times\frac{t^4}{3!}. \quad (29)$$

We obtained f_n^1: 10 20 4 2.

c. Third Iteration

If f_n^1 and r_n^1 are given, as
$f_n^1: 10\ \ 20\ \ 4\ \ 2,\ r_n^1: 4\ \ 14\ \ 166\ \ 443,\ p_n^1 = 26r_n^1 + f_n^1.$
Let

$$[-f_n^0\{\frac{d^3}{ds^3}(L(\frac{1}{(t-1)^2}))\}] = \sum_{n=0}^{\infty}\frac{p_n^1}{s^{n+4}}$$
$$= \frac{114}{s^4}+\frac{384}{s^5}+\frac{4320}{s^6}+\frac{11520}{s^7}. \quad (30)$$

Taking inverse Laplace transform of (30),

$$f_n^0\frac{u^3}{(1-u)^2} = 114\times\frac{u^3}{3!}+384\times\frac{u^4}{4!}+4320\times\frac{u^5}{5!}+11520\times\frac{u^6}{6!}. \quad (31)$$

Then taking inverse Elzaki transform of (31)

$$E^{-1}\left[f_n^0\frac{u^3}{(1-u)^2}\right] = 19\text{u}^3+16u^4+36u^5+16u^6$$
$$= 19\text{t}+16\times\frac{t^2}{2!}+36\times\frac{t^3}{3!}+16\times\frac{t^4}{4!}$$
$$= 19\text{t}+8\text{t}^2+12\times\frac{t^3}{2!}+4\times\frac{t^4}{3!}. \quad (32)$$

Hence the coded message is 19 8 12 4, that is 'TIME'.
This method is summarized as following theorems:

Theorem 3.3

The given cipher text in the form of $f_n^3,\ n=0,\ 1,\ 2,\ \ldots..$ and key r_n^3 .Let

$$\{-f_n^2[\frac{d^3}{ds^3}(L(\frac{1}{(t-1)^2}))]\}=\sum_{n=0}^{\infty}\frac{p_n^3}{s^{n+4}},\ p_n^3=0\ \forall n\geq 4, \quad (33)$$

then taking inverse Laplace transform of (33)

$$\frac{f_n^2u^3}{(1-u)^2}=\sum_{n=0}^{\infty}\frac{p_n^3u^{n+3}}{(n+3)!}, \quad (34)$$

and then taking inverse Elzaki transform of (34) we get,

$$\mathrm{E}^{-1}\left(\frac{f_n^2u^3}{(1-u)^2}\right)=\sum_{n=0}^{\infty}\frac{f_n^2t^{n+1}}{n!}, \quad (35)$$

where,

$$f_n^2=\frac{p_n^3}{(n+1)\left[(n+3)!\right]},n=0,1,2,\ldots.$$

$$=\frac{26r_n^3+f_n^3}{(n+1)\left[(n+3)!\right]},\ n=0,1,2,\ldots. \quad (36)$$

We obtained f_n^2. Apply the above same procedure on f_n^2 and then on f_n^1, required f_n^0 is obtained.

Theorem 3.4

The given cipher text in the format of f_n^j and key $r_n^j,\ n=0,1,2,..$ and $j=1,2,3,..$ converted into plain text f_n^{j-1}.

Let

$$\{-f_n^{j-1}[\frac{d^3}{ds^3}L(\frac{1}{(t-1)^2})]\}=\sum_{n=0}^{\infty}\frac{p_n^j}{s^{n+4}},$$

$$p_n^j=0,\ \forall n\geq 4. \quad (37)$$

Then taking inverse Laplace transform of (37),

$$\frac{f_n^{j-1}u^3}{(1-u)^2}=\sum_{n=0}^{\infty}\frac{p_n^ju^{n+3}}{(n+3)!}, \quad (38)$$

and taking inverse Elzaki transform of (38).

$$\mathrm{E}^{-1}\left(\frac{f_n^{j-1}u^3}{(1-u)^2}\right)=\sum_{n=0}^{\infty}\frac{f_n^{j-1}t^{n+1}}{n!}, \quad (39)$$

where,

$$f_n^{j-1}=\frac{p_n^j}{(n+1)\left[(n+3)!\right]},n=0,1,2,\ldots..$$

Hence we obtained plain text f_n^{j-1}.

$$=\frac{26r_n^j+f_n^j}{(n+1)\left[(n+3)!\right]},\ j=1,2,\ldots., \quad (40)$$

In our method we use three iterations. Hence for decryption we apply above procedureon f_n^3 for getting f_n^2, then on f_n^2 for getting f_n^1, then on f_n^1 for getting f_n^0.

Conclusions

Cryptographic technique is essential inauthentication, integrity, confidentiality. In the present paper we developed a new iterative method using Laplace and Elzaki transforms for security purpose. In the presented method more number of iterations implies more difficulty in tracing key which increase level of security of message.As compare to other cryptographic methods our method is more secure and strong for encryption as well as decryption since we protect the data with number of iterations..

References

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

[2] ElzakiT. M, "The new Integral TransformElzaki Transform," Global Journal of Pure andApplied mathematics,Vol-.7, 2011.

[3] G. Naga Lakshmi, B. Ravi Kumar and A. ChandraSekhar, "A cryptography scheme of Laplace transforms," International Journal of Mathematics Archive, 2:2515-519,2011.

[4] Patil N. A.and Patil N. V., "Application of Laplace Transform,"Globaljournal of science Research mathematics and decisionScience,2249-4626, vol-12, 2012.

[5] Hiwarekar, A. P., "Application of Laplace Transform For Cryptographic Scheme"Proceeding of the World Congress onEngineering ,95-100, 2013.

[6] Hiwarekar A. P., "New MathematicalModelling for Cryptography,"86' Journal ofInformation Assurance and Security, MIR Lab USA, 9:027-033, 2014.

[7] Hiwarekar A. P., "Cryptography Using Laplace Transform, International Journal of Engineering Research and Applications

Vol.5, Issue 4 (Part-5), 102-106, April 2015.

[8] Sukhija D., "Performance evaluation of cryptographic algorithm: AES and DES," International journal of computer science and mobile computing, Vol-3,Issue 9, pp. 582-585, 2014.

[9] Raisinghania M. D., Advanced differentialEquations, S. Chand and Company, New- Delhi 2015.

[10] MampiSaha, "Application of Laplace – Mellin transform for Cryptography," Rai journal of technology and innovation, Vol-5,Issue 1, 2017.

[11] Roberto P. Briones, "Modification of an encryption scheme based on the Laplace Transform," International journal of current research, vol-10, issue, 07, July, 2018.

[12] P. L.Chitraand K. Sathya, "A novel password encryption using wedgesalgorithm with QR code,"International journal of pure and applied mathematics, Volume 119, 857-861, 2018