CRYPTOGRAPHIC METHOD BASED ON LAPLACE-ELZAKI TRANSFORM

Article · July 2021

2 authors:

Shaila shivaji Jadhav
Tuljaram Chaturchand College

Anil Hiwarekar
Vidya Pratishthan's Kamalnayan Bajaj Institute of Engineering and Technology, B…

CRYPTOGRAPHIC METHOD BASED ON LAPLACE-ELZAKI TRANSFORM

Jadhav Shaila Shivaji Ph. D. Scholar, Shri. J. J. T. University, Rajasthan, India
Email ID: shailajadhavbhosale@gmail.com
Hiwarekar A. P. Vidya Pratishthans Kamalnayan Bajaj Institute of Engineering and Technology, Baramati, India (SPPU Pune) Email ID: hiwarekaranil@gmail.com

ABSTRACT: Protection of hiding information is an essential part in authentication system. Cryptography is technique to protect secrete information such as: various money transfer applications, ATM transaction, online banking etc. where security is the most essential. Cryptography is useful to secure secrete information from unauthorised users. In some cryptographic techniques the Laplace integral transforms and its inverse integral transforms are applicable. In this paper we developed new technique for Cryptography using both Laplace and Elzaki transform.
Key words: Encryption and Decryption, Laplace transform, Elzaki transform, Cryptography.

1. INTRODUCTION

In many situation sender want to hide the message from public or unauthorised used, for this purpose sender encrypt message. Encryption is process to protect information while decryption is process to unlock original message. In literature survey there are various techniques of cryptography based on mathematics. There are various applications of integral transforms in many fields including cryptography. In cryptography Laplace transform, Elzaki transform, Kamal transform are used on sine hyperbolic, cosine hyperbolic, exponential, polynomial function, etc. Cryptographic method using Laplace transform found in Gencoglu M. [3]; Hiwarekar A. P. [4, 5, 6, 7, 8, 9, 10]; Jadhav and Hiwarekar[15]; Roberto P. Briones [11] while use of Elzaki transform found in Bhuvaneswari K. and Bhuvaneswari R. [1]; Sharjeel S. and Barakzai M. [12]; Tarig Elzaki [13]; Undegaonkar and Ingle [14].

Here we use combination of both Laplace and Elzaki transforms for the encrypting message and its inverse transform for decryption.

2. DEFINITIONS

2.1: A text message is converted into another form using suitable technique then resulting converted form is called as cipher text.
2.2: The procedure to encoding the message into cipher text is called as encryption.
2.3: The procedure for decoding message is called as decryption.
2.4: The Laplace Transform:
If $f(t)$ is function of $t > 0$, then Laplace transform of $f(t)$ is denoted as $L\{ f(t)\}$,
and $L\{f(t)\} = \int_0^\infty e^{-st} f(t)dt = F(s)$, provided integral exist.
2.5: Inverse Laplace Transform:
If $L\{ f(t) \} = F(s)$ then Inverse Laplace transform of $F(s)$ denoted by $L^{-1}\{F(s)\} = f(t)$.
2.6: Linearity Property of Laplace Transform:
If $f(t)$ and $g(t)$ are two functions of t and a, b are constants then

$$L\{af(t) + bg(t)\} = aL\{f(t)\} + bL\{g(t)\}.$$

2.7: Linearity Property of Inverse Laplace Transform:
If $L\{f(t)\} = F(s)\ and\ L\{g(t)\} = G(s)$ then $L^{-1}\{F(s) + G(s)\} = L^{-1}\{F(s)\} + L^{-1}\{G(s)\}$.
2.8: Exponential Order:
A function $f(t)$ is said to be of exponential order α as $t \to \infty$ if ∋ constants M > 0, K > 0 such that, $|f(t)| \le Ke^{\alpha t}$, $\forall t > M$.

2.9: Piecewise Continuous Function:

A function $f(t)$ is said to be piecewise continuous on [a, b], if it is defined and continuous on [a, b] except for a finite number of points $t_1, t_2, \dots\dots, t_m$ at each of which left and right limits of $f(t)$exist.

2.10: Elzaki transform:

Elzaki transform of function $f(t)$ which is piecewise continuous and of exponential order is denoted by $E\{f(t)\}$ and defined as $E\{f(t)\} = T(v) = v\int_0^\infty f(t)e^{\frac{-t}{v}}dt,\ t \geq 0, k_1 \leq v \leq k_2$.

2.11: Inverse Elzaki transform:

If $E\{f(t)\} = T(v)$, then Inverse Elzaki transform of $T(v) = f(t)$.
Denoted by $E^{-1}\{T(v)\} = f(t)$.

2.12: Laplace transform and Inverse Laplace transform of some standard functions:

1) $L\{t^n\} = \frac{n!}{s^{n+1}}$, $s > 0$, n is positive integer.
2) $L^{-1}\left\{\frac{n!}{s^{n+1}}\right\} = t^n$, n is positive integer.

2.13: Elzaki transform and Inverse Elzaki transform of some functions:

1. $E\{t^n\} = n!\,u^{n+2}$, n ∈ N.
2. $E\{te^{at}\} = \frac{u^3}{(1-au)^2}$.
3. $E^{-1}\{v^{n+2}\} = \frac{t^n}{n!}$, n ∈ ℕ.

3. CRYPTOGRAPHY TECHNIQUE

3.1: Encryption: Let function $f(t) = F_n te^t = \sum_{n=0}^{\infty} F_n \frac{t^{n+1}}{n!}$ **.**

In this technique the message which is to be encrypted is treated as coefficient of f (t) located as F_n and numbering them 0 to 25 in alphabetical order,
$A = 0,\ B = 1,\ C = 2,\ D = 3,\ E = 4,\ F = 5,\ G = 6,\ H = 7,\ I = 8,\ J = 9,\ K = 10,\ L = 11,$ $M = 12,\ N = 13,\ O = 14,\ P = 15,\ Q = 16,\ R = 17,\ S = 18,\ T = 19,\ U = 20,\ V = 21,\ W = 22,\ X = 23,\ Y = 24,\ Z = 25.$
Example: Let given plain text be INTELLIGENCE,
Hence $F_0 = 8, F_1 = 13, F_2 = 19, F_3 = 4, F_4 = 11, F_5 = 11, F_6 = 8, F_7 = 6, F_8 = 4, F_9 = 13, F_{10} = 2, F_{11} = 4$, and
$f(t) = F_n te^t$ becomes

$$f(t) = \sum_{n=0}^{\infty} F_n \frac{t^{n+1}}{n!}.$$

$$f(t) = [F_0 t + F_1 t^2 + F_2\frac{t^3}{2!} + F_3\frac{t^4}{3!} + F_4\frac{t^5}{4!} + F_5\frac{t^6}{5!} + F_6\frac{t^7}{6!} + F_7\frac{t^8}{7!} + F_8\frac{t^9}{8!} + F_9\frac{t^{10}}{9!} + F_{10}\frac{t^{11}}{10!} + F_{11}\frac{t^{12}}{11!}]$$

, $F_n = 0, n \geq 12$.

$$f(t) = [8t + 13t^2 + 19\frac{t^3}{2!} + 4\frac{t^4}{3!} + 11\frac{t^5}{4!} + 11\frac{t^6}{5!} + 8\frac{t^7}{6!} + 6\frac{t^8}{7!} + 4\frac{t^9}{8!} + 13\frac{t^{10}}{9!} + 2\frac{t^{11}}{10!} + 4\frac{t^{12}}{11!}]$$

,$F_n = 0, n \geq 12$.

3.1.1: First Iteration:

Taking Elzaki transform of $f(t)$,

$E\{f(t)\} = E\{F_n te^t\}$,

$E\{f(t)\} = F_n \frac{u^3}{(1-u)^2}$,

$$E\{f(t)\} = [8u^3 + 13(2!)\,u^4 + \frac{19}{2!}(3!)\,u^5 + \frac{4}{3!}(4!)\,u^6 + \frac{11}{4!}(5!)\,u^7 + \frac{11}{5!}\,(6!)\,u^8 + \frac{8}{6!}\,(7!)\,u^9 + \frac{6}{7!}\,(8!)\,u^{10} + \frac{4}{8!}\,(9!)\,u^{11} + \frac{13}{9!}\,(10!)\,u^{12} + \frac{2}{10!}\,(11!)\,u^{13} + \frac{4}{11!}\,(12!)\,u^{14}]$$

3.1.2: Second Iteration:

Treating u as variable with $u > 0$ in $E\{f(t)\}$ and applying Laplace transform on $E\{f(t)\}$,

$$L\{E\{f(t)\}\} = L\left[F_n \frac{u^3}{(1-u)^2}\right]$$

$$= [\frac{48}{s^4} + \frac{624}{s^5} + \frac{6840}{s^6} + \frac{11520}{s^7} + \frac{277200}{s^8} + \frac{2661120}{s^9} + \frac{20321280}{s^{10}} + \frac{174182400}{s^{11}} + \frac{1437004800}{s^{12}} + \frac{62270208000}{s^{13}} + \frac{136994457600}{s^{14}} + \frac{4184557977600}{s^{15}}] ,u \neq 1.$$

We get coefficient P_n , $n = 0\ to\ 11$.

P_n: 48, 624, 6840, 11520, 277200, 2661120, 20321280, 174182400, 1437004800, 62270208000, 136994457600, 4184557977600.

Consider, $F'_n \equiv P_n mod(26)$ then F'_n: 22 0 2 2 14 20 18 2 10 0 0 0

For n=0 to 11 respectively.

Hence Encrypted message or cipher text is,

WACCOUSCKAAA with key r_n : 1 24 263 443 10661 102350 781587 6699323 55269415 2395008000 5269017600 160944537600,

And $r_n = \frac{P_n - F'_n}{26}$, n = 0 to 11.

3.2: Decryption:

Now given cipher text WACCOUSCKAAA and key r_n.

Equivalent coefficient alphabetical order of cipher text is

F'_n: 22 0 2 2 14 20 18 2 10 0 0 0 r_n : 1 24 263 443 10661 102350 781587 6699323 555269415 2395008000 52690117600 160944537600.

$P_n = 26r_n + F'_n, n = 0\ to 11$ and $P_n = 0\ for\ n \geq 12$.

Let, [-F_n $\{\frac{\partial^3}{\partial s^3} L(\frac{1}{(t-1)^2})\}$] $= \sum_{n=0}^{\infty} \frac{P_n}{s^{n+4}}$

$$=[\frac{48}{s^4} + \frac{624}{s^5} + \frac{6840}{s^6} + \frac{11520}{s^7} + \frac{277200}{s^8} + \frac{2661120}{s^9} + \frac{20321280}{s^{10}} + \frac{174182400}{s^{11}} + \frac{1437004800}{s^{12}} + \frac{62270208000}{s^{13}} + \frac{136994457600}{s^{14}} + \frac{4184557977600}{s^{15}}] , t\neq 1.$$

3.2.1: First Iteration:

Taking inverse Laplace of previous equation we get

$$F_n \frac{u^3}{(1-u)^2} = [8u^3 + 26u^4 + 57u^5 + 16u^6 + 55u^7 + 66u^8 + 56u^9 + 48u^{10} + 36u^{11} + 130u^{12} + 22u^{13} + 48u^{14}].$$

3.2.2: Second Iteration:

Taking inverse Elzaki transform of equation obtained in first iteration,

$$E^{-1}\left(\frac{F_n u^3}{(1-u)^2}\right) = [8t + 13t^2 + 19\frac{t^3}{2!} + 4\frac{t^4}{3!} + 11\frac{t^5}{4!} + 11\frac{t^6}{5!} + 8\frac{t^7}{6!} + 6\frac{t^8}{7!} + 4\frac{t^9}{8!} + 13\frac{t^{10}}{9!} + 2\frac{t^{11}}{10!} + 4\frac{t^{12}}{11!}].$$

Hence F_n: 8 13 19 4 11 11 8 6 4 13 2 4, and message is INTELLIGENCE.

In above technique we use $(EL)^{-1} = L^{-1}E^{-1}$ for Laplace (L) and Elzaki (E) transforms.

The above Encryption and Decryption included in the following Theorem:

Theorem 3.1: The given plain text in terms of $F_n, n = 0, 1, 2, 3$ … … … … …under Elzaki transform of $f(t) = F_n te^t$,

$E\{F_n te^t\} = \sum_{n=0}^{\infty} q_n u^{n+3}$, Where $q_n = F_n(n+1)$ and then Laplace transform of {E(f(t))} which is $\sum_{n=0}^{\infty} \frac{P_n}{s^{n+4}}$ where $P_n = (n+1)(n+3)!\, F_n$ and $(1+n)(n+3)!\, F_n \equiv F'_n mod(26)$,

key $r_n = \frac{P_n - F'_n}{26}, n = 0\ to\ 11$.

Theorem 3.2: The given cipher text F'_n and key r_n.

Consider, $F_n\left(-\frac{\partial^3}{\partial s^3} L\left(\frac{1}{(t-1)^2}\right)\right) = \sum_{n=0}^{\infty} \frac{P_n}{s^{n+4}} - - - (I)$

Where $P_n = 26r_n + F'_n, n = 0, 1, 2, ...$
Taking Inverse Laplace transform of (I) which is,
$$\frac{F_n u^3}{(1-u)^2} = \sum_{n=0}^{\infty} \frac{P_n}{(n+3)!} u^{n+3} - - - (II)$$
Taking Inverse Elzaki transform of (II) obtained, $F_n t e^t = \sum_{n=0}^{\infty} F_n \frac{t^{n+1}}{n!}$
Where $F_n = \frac{26r_n + F'_n}{(n+1)(n+3)!}, n = 0, 1, 2 ....$ are in required alphabetical order of plain text.

4. GENERALIZATION

We generalized our result on $F_n t e^t$ to $F_n t^j e^{at}$, $j, a \in$ N Taking Elzaki transform in first iteration we obtain coefficients $q_n = a^n F_n (n+j)(n+j-1)(n+j-2) \dots \dots \dots (n+1)$
In second iteration taking Laplace transform to obtain coefficients,
$P_n = a^n F_n (n+j)(n+j-1)(n+j-2) \dots \dots \dots (n+1)(n+2+j)!, j, a \in$ N
and convert given plain message F_n into F'_n with,
$F'_n = a^n F_n (n+j)(n+j-1)(n+j-2) \dots \dots \dots (n+1)(n+2+j)! \, mod(26)$
$= P_n mod(26), j, a \in$ N,
Where $P_n = a^n F_n (n+j)(n+j-1)(n+j-2) \dots \dots \dots (n+1)(n+2+j)!$
And key $r_n = \frac{P_n - F'_n}{26}$, $n = 0,1,2 \dots ..$ $and\ j, a \in$ N.
For decryption process,
Consider received message F'_n and given key r_n.
Let $F_n \left(-\frac{\partial^3}{\partial s^3} L\left(\frac{1}{(t-1)^2}\right)\right) = \sum_{n=0}^{\infty} \frac{P_n}{s^{n+3+j}}$,
If $P_n = 26r_n + F'_n$ after Taking Inverse Laplace transform we obtain
G(u) $=\sum_{n=0}^{\infty} \frac{P_n}{(n+2+j)!} u^{n+2+j}$.

In second iteration taking Inverse Elzaki transform get,
$F_n t^j e^{at} = \sum_{n=0}^{\infty} F_n \frac{a^n t^{n+j}}{n!}$,
$F_n = \frac{26r_n + F'_n}{(n+2+j)!(n+j)(n+j-1)\dots\dots(n+1)}$, $r_n = \frac{P_n - F'_n}{26}$, $n = 0,1,2,3 \dots$
These generalized result expressed in following theorems.
Theorem 4.1 – The given plain text in terms of coefficients, F_n for n = 0, 1, 2, 3…
Under Elzaki transform of $F t^j e^{at}, j, a \in$ N.
We obtain $q_n = a^n F_n (n+j)(n+j-1)(n+j-2) \dots \dots \dots (n+1)$.
and applying Laplace transform of resulting equation in first obtain coefficient
$P_n = a^n F_n (n+j)(n+j-1)(n+j-2) \dots \dots \dots (n+1)(n+2+j)!$.
And required cipher text is
$F'_n = a^n F_n (n+j)(n+j-1)(n+j-2) \dots \dots \dots (n+1)(n+2+j)! \, mod(26) \equiv P_n mod(26)$, $j, a \in$ N.
With key $r_n = \frac{P_n - F'_n}{26}$, n = 0, 1, 2….
Theorem 4.2: Consider cipher text F'_n and key r_n with
$F_n \left(-\frac{\partial^3}{\partial s^3} L\left(\frac{1}{(t-1)^2}\right)\right) = \sum_{n=0}^{\infty} \frac{P_n}{s^{n+3+j}}$ -- (III)
If, $P_n = 26r_n + F'_n$
After inverse Laplace transform of (III) and then inverse Elzaki transform we obtain original message,
$F_n t^j e^{at} = \sum_{n=0}^{\infty} F_n \frac{a^n t^{n+j}}{n!}$, $a, j \in$ N
$F_n = \frac{26r_n + F'_n}{(n+2+j)!(n+j)(n+j-1)\dots\dots(n+1)}$ and $r_n = \frac{P_n - F'_n}{26}$, $n = 0, 1, 2, 3 \dots.$

5. ILLESTRATIVE EXAMPLES

Suppose plain text is GOOD,
Using technique explained in section 3,
That is j = 1, a = 1 for function $F_n t^j e^{at}$

Cipher text is KWWI.

5.1 If j = 4, a = 10, cipher text is SKIW.
5.2 If j = 3, a = 9, cipher text is EOIY.
5.3 If j = 2, a = 8, cipher text is COSW.
5.4 If j = 1, a = 7, cipher text is KYMO.

6. CONCLUDING REMARK

In many situations such as e-services, banking transactions, military secrete or coding language is essential for security purpose. In present paper we introduce new technique using both Laplace and Elzaki transform for encryption and its Inverses for decryption. Using combination of two integral transforms increases level of security in decryption of the message. It is applicable in prevention of fraud in various systems in which coding or cryptography is used. The work can be extendable further by choosing new function and changing other components in it.

REFERENCES:

[1] Bhuvaneswari K. and Bhuvaneswari R., Application of Tarig transform in Cryptography, International Journal of creative research thoughts, Vol. 8, Issue 6, pp. 1878-1880, (June 2020).
[2] Debnath L. and Bhatta D., Integral transforms and their Applications, Chapman and Hall/CRC, First Indian edn., 2010.
[3] Gencoglu M., Cryptanalysis of a new method of Cryptography using Laplace transform Hyperbolic functions, Communications in Mathematics and applications, Vol. 8, Issue 2, pp. 183-189, (2017).
[4] Hiwarekar A.P., A new method of cryptography using Laplace transform, International Journal of Mathematical Archive, 3(3), pp 1193-1197, (2012).
[5] Hiwarekar A.P., A new method of cryptography using Laplace transform of hyperbolic Functions, International Journal of Mathematical Archive, 4(2), pp 208- 213, (2013).
[6] Hiwarekar A.P., Application of Laplace transform for Cryptographic Scheme, Proceeding of World Congress on Engineering, Vol. II, LNCS, pp 95-100, (2013).
[7] Hiwarekar A.P., Application of Laplace transform for Cryptography, International Journal of Engineering & Science Research, Vol-5, Issue-4, pp 129-135, (April 2015).
[8] Hiwarekar A.P., Cryptography Using Laplace transform, Int. Journal of Engineering Research and Applications, Vol. 5, Issue 4, (Part -5), pp.102-106, (April 2015).
[9] Hiwarekar A.P., Encryption-Decryption Using Laplace transforms, Asian Journal of Mathematics and Computer Research, International Knowledge Press, Vol.12, (3), pp.201-209, (2016).
[10] Hiwarekar A. P., New Mathematical Modeling for Cryptography, Journal of Information Assurance and Security, MIR Lab USA, Vol. 9, pp. 027-033, (2014).
[11] Roberto P. Briones, Modification of an encryption scheme based on the Laplace Transform, International journal of current research, Vol. 10, issue 7, pp. 71759-71763, (July 2018).
[12] Sharjeel S. and Barakzai M., Some new applications of Elzaki transform for solution of Linear Volterra Type Integral Equations, Journal of Applied Mathematics and Physics, Vol. 7, Issue 08, pp. 1877-1892, (Aug 2019).
[13] Tarig. M. Elzaki, The new Integral transform Elzaki transform, Global Journal of Pure and Applied Mathematics, Vol. 7, Issue 1, pp. 57-64, (Jan 2011).
[14] Undegaonkar H. and Ingle R., Role of some Integral transforms in Cryptography, International Journal of Engineering and advanced Technology, Vol. 9, Issue 3, pp. 376-380, (Feb 2020).
[15] Jadhav S. and Hiwarekar A., New Method for Cryptography using Laplace-Elzaki Transform, Psychology and Education, Vol. 58, Issue 5, pp. 1-6, (April 2021).