An Application of the Elzaki Transform in Cryptography

Uttam Dattu Kharde

Asst. Professor, Dept. of Mathematics,
S.N.Arts, D.J.M. Commerce & B.N.S. Science College, Sangamner, MS (India).
Email: uttamkharde@gmail.com

ABSTRACT.

Cryptography is the science of transmission and reception of secrete message. It has been used for providing secure communication between individuals In this paper author proposed a new method of cryptography, in which new integral transform “Elzaki Transform” is used for encrypting the plain text message and corresponding inverse transform for Decryption.

KEYWORD: Cryptography, Encryption, Decryption, Elzaki transform.

1. INTRODUCTION

In the present day, electronic communication such as mobile communication, e-banking, e-commerce, financial information, ATM cards, emails, etc has become an essential part of every aspect of human life. With the growing quantity of digital data stored and communicated by electronic data-processing system, it is necessary to protect information from unwanted intrusion [1]. Cryptography is the science of transmission and reception of secrete message. It has been used for providing secure communication between individuals [3, 4, 5, 6].

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. The communication security is gaining importance as a result of the more and more use of electronic communication in day to day activities. Cryptography is the most important tool that provides network security during electronic communication. Encryption is the process of converting or encoding original information in such a way that only authorized person can access. This is usually done for secrecy and typically for confidential communication [1, 2].

A cipher is an algorithm for performing encryption and decryption [1]. The original information is called plain text and the encrypted form as cipher text. The cipher text contains all the information of the plain text message but is not in a format readable by human or computer without proper mechanism to decrypt it. Ciphers are usually parameterized by a piece of auxiliary information called a Key [3]. The encryption procedure is varied depending on the key, which changes the detailed operation of the algorithm. Without the appropriate key the decryption is highly impossible [1, 2, 3, 4, 5, 6].

In the present paper a new cryptographic method is planned in which Elzaki transform is used for encrypting the plain text and corresponding inverse transform is used for decryption. Elzaki transform was introduced by Tarig M. Elzaki in 2011 and is widely used in applied mathematics as well as in engineering field [7, 8, 9, 10, and 11]. The plan of the paper is as follows: In section 2, we introduce definition and some standard results of Elzaki transforms, proposed method & illustrative example in 3, and conclusion in 4.

2. DEFINITION AND SOME STANDARD RESULTS

2.1. Elzaki transform:

A new integral transform called the Elzaki transform defined for the function of exponential order, we consider functions in the set A defined by [7]

$$A = \{f(t) : \exists M, k_1, k_2 > 0, |f(t)| < M e^{\frac{|t|}{k_j}}, \text{i} f t \in (-1)^j \times [0, \infty)\} \qquad (1)$$

For a given function in the set A, the constant M must be finite number, k_1, k_2 may be finite or infinite.
The Elzaki transform of the function $f(t) \in A$, denoted by $E[f(t)]$ or $T(v)$, is defined by the integral equation [7, 8],

$$E[f(t)] = T(v) = v \int_0^\infty f(t) e^{\frac{-t}{v}} dt, \forall\, t \geq 0, k_1 \leq v \leq k_2 \qquad (2)$$

The function $f(t)$ in equ. (2) is called the inverse Elzaki transform of $T(v)$ and is denoted by $f(t) = E^{-1}[T(v)]$.
We use the following standard results of Elzaki transform [7, 8, 9, 10, 11].

2.2. Linear property: Elzaki transform is a linear transform.

That means, if $E[f_1(t)] = T_1(v)\ akd\ E[f_2(t)] = T_2(v)$ then $E[c_1 f_1(t) + c_2 f_2(t)] = c_1 T_1(v) + c_2 T_2(v)$, where c_1 & c_2 are constants.

2.3. Elzaki transform of some elementary functions:

i) $E[1] = v^2 \qquad \therefore E^{-1}[v^2] = 1$

ii) $E[t^n] = k!\, v^{n+2} \qquad \therefore E^{-1}[v^{n+2}] = \frac{t^n}{n!} \quad \forall k = 1,2,3, \ldots$

iii) $E[e^{at}] = \frac{v^2}{1-av} \qquad \therefore E^{-1}\left[\frac{v^2}{1-av}\right] = e^{at}$

3. PROPOSED METHOD

The following algorithm provides the proposed cryptographic method. The sender converts the information in to cipher text using following steps [1, 2]:

3.1. Encryption:

i) Assign every letter in the plain text as a number in such a way that $A = 1, B = 2, C = 3, \ldots Z = 26\ akd\ [space] = 0$.
Thus our original message is converting in to a finite sequence of numbers.
For example, plain text "MATHEMATICS" is converted in to a finite sequence $13, 1, 20, 8, 5, 13, 1, 20, 9, 3, 19$.

ii) If n is the number of terms in the sequence, then consider a polynomial $f(t)$ of degree (n-1) with coefficients as the term of the given finite sequence.
In previous example, sequence contains 11 terms, so $f(t)$ is a polynomial of degree 10 as follows:
$f(t) = 13 + t + 20t^2 + 8t^3 + 5t^4 + 13t^5 + t^6 + 20t^7 + 9t^8 + 3t^9 + 19t^{10}$

iii) Apply Elzaki transform to $f(t)$ i. e. $T(v) = E[f(t)]$
Thus, in above example
$T(v) = 13v^2 + v^3 + 4v^4 + 48v^5 + 120v^6 + 1560v^7 + 720v^8 + 100800v^9 + 362880v^{10} + 1088640v^{11} + 68947200v^{12}$

$$\therefore T(v) = \sum_{i=1}^{11} c_i v^{i+1} \qquad (3)$$

iv) For each i, find quotient q_i and remainder r_i such that $c_i = 26q_i + r_i$. Hence the finite sequence $q_1, q_2, q_3, \ldots, q_n$ forms the Key [1, 2].
Thus in above we have,

$c_1 = 13 = 26 \times 0 + 13 \qquad c_2 = 1 = 26 \times 0 + 1$

$c_3 = 4 = 26 \times 0 + 4 \qquad c_4 = 48 = 26 \times 1 + 22$

$c_5 = 120 = 26 \times 4 + 16 \qquad c_6 = 1560 = 26 \times 60 + 0$

$c_7 = 720 = 26 \times 27 + 18 \qquad c_8 = 100800 = 26 \times 3876 + 24$

$c_9 = 362880 = 26 \times 13956 + 24\ c_{10} = 1088640 = 26 \times 41870 + 20$

$c_{11} = 68947200 = 26 \times 2651815 + 10$

So the key is 0, 0, 0, 1, 4, 60, 27, 3876, 13956, 41870, 2651815.

v) Consider a new finite sequence of numbers $r_1, r_2, r_3, \dots, r_n$. Using step (i) given in 3.1 convert the numbers of the new sequence in to text called as cipher text [1, 2].

In above example, new finite sequence is 13, 1, 4, 22, 16, 0, 18, 24, 24, 20, 10. Hence cipher text is MADVP RXXTJ.

Thus the original message "MATHEMATICS" is converted in to cipher text "MADVP RXXTJ". The sender publically send the message "MADVP RXXTJ" & $\sum_{i=1}^{11} c_i v^{i+1}$ and privately send the Key & Elzaki transform [3].

3.2. Decryption:

i) Convert the cipher text MADVP RXXTJ in to corresponding finite sequence of numbers $r_1, r_2, r_3, \dots, r_n$ i.e. 13, 1, 4, 22, 16, 0, 18, 24, 24, 20, 10.

ii) Using key q_i and the values of r_i find c_i such that

$c_i = 26q_i + r_i \ \forall \ i = 1,2,3, \dots, k.$

Thus in above example we get,

$c_1 = 26 \times 0 + 13 = 13$ $c_2 = 26 \times 0 + 1 = 1$

$c_3 = 26 \times 0 + 4 = 4$ $c_4 = 26 \times 1 + 22 = 48$

$c_5 = 26 \times 4 + 16 = 120$ $c_6 = 26 \times 60 + 0 = 1560$

$c_7 = 26 \times 27 + 18 = 720$ $c_8 = 26 \times 3876 + 24 = 100800$

$c_9 = 26 \times 13956 + 24 = 362880$ $c_{10} = 26 \times 41870 + 20 = 1088640$

$c_{11} = 26 \times 2651815 + 10 = 68947200$

iii) Let $T(v) = \sum_{i=1}^{n} c_i v^{i+1}$

Thus, $T(v) = 13v^2 + v^3 + 4v^4 + 48v^5 + 120v^6 + 1560v^7 + 720v^8 + 100800v^9 + 362880v^{10} + 1088640v^{11} + 68947200v^{12}$

iv) Apply inverse Elzaki transform to $T(v)$ we get $f(t)$.

Thus, $f(t) = E^{-1}[T(v)] = 13 + t + 20t^2 + 8t^3 + 5t^4 + 13t^5 + t^6 + 20t^7 + 9t^8 + 3t^9 + 19t^{10}$.

v) Then consider the coefficients of $f(t)$ as a finite sequence of numbers

13, 1, 20, 8, 5, 13, 1, 20, 9, 3, 19 .

vi) Using step (i) given in 3.1, we get the original message MATHEMATICS.

4. CONCLUSION

In the proposed work a new cryptographic method is introduced using Elzaki transforms and the private key is the number of multiples of modulo 26. Therefore it is very difficult for an eyedropper to trace the key by any attack.

REFERENCES

[1] Burton D.M. (2002), Elementary Number Theory, Tata McGraw Hill, New Delhi.

[2] Stallings W (2005), Cryptography and Network Security, Prentice Hall (4th Ed.).

[3] D.S. Bodkhe & S.K. Panchal (2015), Use of Sumudu Transform in Cryptography, Bulletin of the Marathwada Mathematical Science, Vol-16, No. 1, pp 1-6.

[4] Hiwarekar A.P. (2012), A new method of Cryptography using Laplace Transform, Intr. J. Math. Arch:3(3), pp. 1193-1197.

[5] G. Naga Lakshmi, B. RaviKumar and A. Chandra Sekhar (2011), A cryptographic Scheme of Laplace Transforms, Intr. J. Math. Arch. 2(12), pp. 2515-2519.

[6] Abdelilah K. Hassan Sedeeg, Mohand M. Abdelrahim Mahgoub and Munner A Saif Saeed (2016), An Application of the New Integral "Aboodh Transform" in Cryptography, Pure and Applied Mathematics Journal, Vol-5, No.5, pp. 151-154.

[7] Tarig M. Elzaki (2011), The New Integral Transform "Elzaki Transform", Global Journal of Pure and Applied Mathematics, Vol-7, No.1, pp. 57-64.

[8] Tarig M. Elzaki, Salil M. Elzaki & E.A. Elnour (2012), On the New Integral Transform "Elzaki Transform" Fundamental Properties Investigations and Applications, Global Journal of Mathematical Sciences: Theory and Practical, Vol- 4, No.1, pp. 1-13.

[9] Tarig M. Elzaki & Salil M. Elzaki (2011), On the connection between Laplace and Elzaki Transforms, Advances in Theoretical and Applied Mathematics, Vol-6, No.1, pp. 1-10.

[10] Tarig M. Elzaki & Salil M. Elzaki (2011), Application of New Integral Transform "Elzaki Transform" to Partial Differential Equations, Global Journal of Pure and Applied Mathematics, Vol-7, No.1, pp. 65-70.

[11] Uttam D. Kharde (2016), The comparative study of the Laplace Transform and New Integral Transform Elzaki Transform, Online International Interdisciplinary Research Journal, ISSN 2249-9598, Vol-6, No-5,pp. 90-93.