International Journal of Engineering & Technology, *12 (2) (2023) 109-111*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Securing data transmission by cryptography using Rohit integral transform

Rohit Gupta [1] *, Rahul Gupta [2]

[1] *Lecturer, Dept. of Applied Sciences (Physics), Yogananda College of Engineering and Technology (YCET), Jammu*
[2] *Lecturer, Dept. of Physics, G.D. Goenka Public School, Jammu*
**Corresponding author E-mail:guprarohit565@gmail.com*

Abstract

The encryption and decryption processes to secure data transmission and protection in cryptography are very useful in a communication system for authentication and privacy. Recently, integral transform techniques have been used by many researchers to increase the strength of encryption and decryption processes in cryptography. In this paper, the ability of Rohit integral transform (RIT) is shown for the encryption and decryption processes in cryptography and in general, in the field of data security through practical application.

Keywords: *Cryptography; Rohit Integral Transform (RIT); Encryption and Decryption Processes.*

1. Introduction

Cryptography is a critical technique to secure data transmission and protection for authentication and privacy [1]. It is a discipline concerned with communication system confidentiality [2]. Recently, researchers have been working to protect and preserve data from penetration by attackers. They are finding new techniques of encryption that are sufficient to protect the data of governmental and non-governmental organizations, where encryption plays an important role in data security and protection [3]. Cryptography enables us to store sensitive information or transmit it over insecure internet networks so that it can only be read by the intended recipient [4]. In the field of cryptography, integral transforms have been applied to the exponential functions of prepositions in encoding and decoding operations [5-9]. In this paper, the Rohit integral transform has been applied in the field of cipher, a method of writing in which a secret pattern of a particular set of letters or symbols is used to represent other letters or symbols [10], for the encoding of a plain text, and then decoding this cipher for obtaining the original text.

The Rohit transform [11], [12] of a function g(t) is defined by the integral equations as $R\{g(t)\} = G(r) = r^3 \int_0^\infty e^{-rt} g(t)dt, t \geq 0 , r_1 \leq r \leq r_2$, provided that the integral is convergent, where r may be a real or complex parameter and R is the integral Rohit Transform operator. The variable r in this transform is used to factor the variable t in the argument of the function g. The integral Rohit transform when applied to a function, changes that function into a new function by using a process that involves integration [13, 14].

The RT of some elementary functions [15] is given by

1) $R\,\{1\} = r^3 \int_0^\infty e^{-rt}\, dt = -r^2(e^{-\infty} - e^{-0}) = -r^2(0-1) = r^2$

Hence $R\,\{1\} = r^2$

2) $R\,\{t^n\} = r^3 \int_0^\infty e^{-rt}\, t^n\, dt = r^3 \int_0^\infty e^{-z} \left(\frac{z}{r}\right)^n \frac{dz}{r}, z = rt$

$$R\,\{t^n\} = \frac{r^2}{r^n} \int_0^\infty e^{-z}\,(z)^n dz$$

Applying the definition of the gamma function,

$$R\,\{t^n\} = \frac{r^2}{r^n} \Gamma(n+1) = \frac{r^2}{r^n} n! = \frac{n!}{r^{n-2}}$$

Hence $R\,\{t^n\} = \frac{n!}{r^{n-2}}$

2. Proposed cryptographic methodology

The steps carried out at the transmission end (where the data is encrypted) are as follows:

- Before beginning the encryption process, the sender and receiver must agree on a key called R Key (say).
- The plain text message is organized as a finite sequence of numbers.

For example, A = 1, B = 2, C = 3, D = 4…….Z = 26.

- If we consider that the number of terms can be represented in the plain text as (t+1), then we can form a polynomial g(t) of degree t with an operand considered as a given sequence term.
- Take the Rohit integral transform of a polynomial obtained above.
- Find the remainders gs such that gs = Qs mod 26, where s = 0, 1, 2…
- The values of remainder gs for all s will be the encrypted message.
- Find the keys Ks such that (Qs- gs)/26= Ks $for\ all$ s = 0, 1, 2…

The steps carried out at the receiver end (where the received data is decrypted) are as follows:

- Consider the cipher text and key received (R Key) from the sender.
- Convert the given cipher text to the corresponding finite sequence of numbers using the given key$s$ Ks ∀ s = 0, 1...., assuming (Qs-gs)/26= Ks $for\ all$ s = 0, 1, 2..…
- Apply the inverse RIT.
- After converting the numbers in the preceding finite sequence to alphabets, the original plain text is obtained.

3. Practical application of RIT in cryptography

Here, the practical application of RIT in cryptography for the encryption and decryption of plain text will be shown.

3.1. Encryption (encoding) stage

This stage is implemented through the transmitter, encryption is applied to the information to convert it from consistent to inconsistent information.
The plain text is transformed into their corresponding serial numbers i.e.

A ≡ 1, B ≡ 2, C ≡ 3, D ≡ 4, ……., Z ≡ 26.

The text is arranged as a bounded series. For instance, the characters of text: RESEARCH are transformed into their corresponding serial numbers:

R ≡ 18, E ≡ 5, S ≡ 19, E ≡ 5, A ≡ 1, R ≡ 18, C ≡ 3, H ≡ 8.

So, the bounded series of the text is: (18, 5, 19, 5, 1, 18, 3, 8).
If we consider that the number of terms can be represented in the plain text as (t+1), then we can form a polynomial g(t) of degree t with an operand considered as a given sequence term. In the given case, the bounded series contains (7+1) terms, so the polynomial g(t) formed is of degree 7 and is written as

$$g(t) = 18+ 5t+ 19t^2+ 5t^3+ 1t^4 + 18t^5 + 3t^6 + 8t^7 .$$

Applying RIT [16, 17] to the above equation, we have

$$G(q)= 18\, q^2+ 5q + 19(2!\, q^0) + 5\,\frac{3!}{q} + \frac{4!}{q^2} + 18\,\frac{5!}{q^3} +3\,\frac{6!}{q4} + 8\,\frac{7!}{q5}$$

$$G(q)= 18q^2+ 5q + 38\, q^0 + \frac{30}{q} + \frac{24}{q2} + \frac{2160}{q3} + \frac{2160}{q4} + \frac{6720}{q5} = \sum_{s=0}^{7} \frac{Q_s}{q^{s-2}} \tag{1}$$

Now finding g_s where $g_s = Q_s$ mod 26 for all s = 0, 1, 2…..7, we have
$g_0 \equiv 18$ mod 26 = 18.
$g_1 \equiv 5$ mod 26 = 5
$g_2 \equiv 38$ mod 26 = 12
$g_3 \equiv 30$ mod 26 = 4
$g_4 \equiv 24$ mod 26 = 24
$g_5 \equiv 2160$ mod 26 = 2
$g_6 \equiv 2160$ mod 26 = 2
$g_7 \equiv 6720$ mod 26 =12

So $Q_s = 26K_s + g_s$. Here the keys K_s for all s = 0, 1, 2…………7 is

$K_0 = 0$, $K_1 = 0$, $K_2 = 1$, $K_3 = 1$, $K_4 = 0$, $K_5 = 83$, $K_6 = 83$, $K_7 = 258$

The encryption operation created a new bounded series as:

$\{g_{0,}\, g_{1,}\, g_2 ......\, g_7\} = \{18, 5, 12, 4, 24, 2, 2, 12\}$

3.2. Decryption (decoding) stage

This stage is implemented on the encrypted text to convert it into consistent information.
The encrypted text is received from the transmitter via a secure route. For instance, the encrypted text, here is RELDXBBL, and the key is {0, 0, 1, 1, 0, 83, 83, 258}.
The received encrypted text is transformed into the equivalent finite sequence of the numbers:

$\{g_{0,} g_{1,} g_{2\ldots\ldots} g_7\} = \{18, 5, 12, 4, 24, 2, 2, 12\}$

Hence $Q_s = 26K_s + g_s$ for all s = 0, 1, 2……..7.

Applying the inverse RIT to the equation (1) i.e.

$G(q)= 18\ q^2+ 5\ q^1 + 19(2!\ q^0) + 5\ \frac{3!}{q} + \frac{4!}{q^2} + 18\ \frac{5!}{q^3} +3\frac{6!}{q^4} + 8\ \frac{7!}{q^5}$, we obtain

$g(t) = 18+ 5t+ 19t^2+ 5t^3+ 1t^4 +18t^5+3t^6+8t^7$

If we look closely at the polynomial coefficients, it is found that we have obtained g(t). They can be considered as finite sequences, and thus the numerals of the above bounded sequence can be converted to their equivalent characters, to get the genuine transmitted text RESEARCH.

4. Discussion and conclusion

In this work, the strength and success of the Rohit integral transform in the field of cipher has been proven, as it was applied in encrypting the plain text and converting it to an unclear cipher text, and when using its inverse proved the ability to return the cipher text to the original understandable text. The proposed work introduces a new cryptographic scheme based on Rohit integral transform (RIT) with a key which is extremely difficult to trace.

References

[1] C. Paar and J. Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. 2010th Edition Springer-Verlag Berlin Heidelberg, (2010). https://doi.org/10.1007/978-3-642-04101-3.

[2] N.S. Mohammed and Emad A. Kuffi. Perform the CSI complex Sadik integral transform in cryptography. *Journal of Interdisciplinary Mathematics*. Vol. 26, No. 6, pp. 1303–1309 (2023). https://doi.org/10.47974/JIM-1628.

[3] H. K. Undegaonkar and R.N. Ingle. Role of Some Integral Transforms in Cryptography. International Journal of Engineering and Advanced Technology, 9, 376-380 (2020). https://doi.org/10.35940/ijeat.C5117.029320.

[4] P.S. Kumer and S. Vasuki. An application of Mahgoub Transform in Cryptography. Advances in Theoretical and Applied Mathematics. 13(2), 91-99 (2018).

[5] V. Srinivas and C.H. Jayanthi. Application of the New Integral J-transform in Cryptography. International Journal of Emerging Technologies. 11 (2), 678-682 (2020).

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

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

[8] Asmaa O. Mubayrash, Huda M. Khalat, New method for cryptography using abaoub- shkheam transform, The Libyan Journal of Science- University of Tripoli, Vol. 25, No. 02, (2022), 35-39.

[9] Abdelilah K. Hassan Sedeeg, Mohand M. Abdelrahim Mahgoub, Muneer A. Saif Saeed, (2016). An Application of the New Integral "Aboodh Transform" in Cryptography, Int J Pure Appl Math, 5 (5), 151-154. https://doi.org/10.11648/j.pamj.20160505.12.

[10] Uttam Dattu Kharde., 2017, "An Application of the Elzaki Transform in Cryptography", Journal for Advanced Research in Applied Sciences, 4(5), pp. 86– 89.

[11] Rohit Gupta, 'On novel integral transform: Rohit Transform and its application to boundary value problems', ASIO Journal of Chemistry, Physics, Mathematics and Applied Sciences (ASIO-JCPMAS), 4(1), 2020, pp. 08-13.

[12] Rohit Gupta, Rahul Gupta, Ajay Kumar, Analysis of Impulsive Response of Mechanical and Electrical Oscillators by Rohit Transform, Engineering and Scientific International Journal (ESIJ), 9(3), 2022, pp. 51-54.

[13] Anamika, Rohit Gupta, Analysis Of Basic Series Inverter Via The Application Of Rohit Transform, International Journal of Advance Research and Innovative Ideas in Education, 6(6), 2020, pp. 868-873.

[14] Rohit Gupta rotu and Ajay Sharma, "Response of Non-Damped Oscillators Subjected To Rectangular Pulse", International Journal of Engineering and Applied Physics, vol. 3, no. 3, pp. 858–864, Oct. 2023.

[15] Rohit Gupta, Inderdeep Singh, Ankush Sharma, Response of an Undamped Forced Oscillator via Rohit Transform, International Journal of Emerging Trends in Engineering Research, Volume 10. No.8, 2022, pp. 396-400. https://doi.org/10.30534/ijeter/2022/031082022.

[16] Rohit Gupta, and Inderdeep Singh, "Analysis of One-Way Streamline Flow Between Parallel Plates Via Rohit Integral Transform," International Journal of Trendy Research in Engineering and Technology, vol. 6, no. 5, 2022, pp. 29-32.

[17] Rohit Gupta, Rahul Gupta, and Anamika Singh, "Response of a Permanent Magnet Moving Coil Instrument via the Application of Rohit Transform," Engineering and Scientific International Journal (ESIJ), vol. 8, no. 2, 2021, pp. 42-44.