Ibn Al-Haitham Journal for Pure and Applied Sciences
Journal homepage: jih.uobaghdad.edu.iq
PISSN: 1609-4042, EISSN: 2521-3407
IHJPAS. 2024, 37(3)

Cryptography In Communication System Via Gupta Integral Transform

Rahul Gupta[1], Rohit Gupta[2*] and Dinesh Verma[3]
[1]Department of Physics, G.D. Goenka Public School, University of Jammu, India.
[2]Department of Applied Sciences (Physics), Yogananda College of Engineering and Technology (YCET), University of Jammu, India.
[3]Department of Mathematics, NIILM University, Kaithal, Haryana, India.
*Corresponding Author.

Received:26 December 2023 Accepted:13 March 2024 Published:20 July 2024
doi.org/10.30526/37.3.3875

Abstract

Cryptography is a critical approach to secure data transmission and protection for authentication and privacy. It is a discipline related with communication system confidentiality. Recently, integral transform approach has been employed by many researchers to increase the power of encryption and decryption processes in cryptography. A group of practices known as information security are meant to stop unwanted access or changes to data. Cryptography is the sole thing preventing the hacker from reading protected data if they are able to bypass the security firewall, passwords, and other precautions put in place to keep them out. Thus, cryptography aids in data protection for both individuals and organizations. In order to prevent the ciphertext from being utilized for plaintext replication without the corresponding key, cryptography aims to transform plaintext into ciphertext that may be communicated across insecure communication channels. The number of multiples of mod n serves as the key in the newly designed cryptographic technique in the proposed work, which makes use of the Gupta transform. As a result, any kind of attack by an eyedropper finding the key would be exceedingly tough. The integral Gupta transform uses the symmetric cryptosystem where the key must stay secret and shared between the involved parties only to encrypt the transmitted plaintext. The Inverse integral Gupta transform is used to decrypt the received ciphertext back into its original context. The ability of integral Gupta transform is exhibited for the encryption and decryption processes in cryptography and in general, in the area of data security with the help of a practical application.

Keywords: Cryptography, integral Gupta transform, Encryption and Decryption Processes.

1. Introduction

Cryptography, a discipline concerned with safeguarding communication and information from hostile forces, serves as an indispensable component in multiple facets of contemporary existence. Such areas encompass the protection of electronic transactions, the preservation of delicate data, and the assurance of privacy in communication [1, 2]. At its essence, cryptography entails the conversion of plaintext (ordinary, comprehensible information) into ciphertext (illegible data) through the utilization of cryptographic algorithms and keys [3, 4].

The principal aims of cryptography encompass confidentiality, integrity, authentication, and non-repudiation. Cryptography relies on cryptographic algorithms, which are mathematical functions designed to perform encryption and decryption operations. These algorithms can be symmetric or asymmetric. In the realm of symmetric cryptography, the identical key is employed for both the process of encryption and decryption. This approach proves to be efficient when dealing with sizable quantities of data, although it necessitates a secure methodology for the exchange of keys between the parties engaged in communication. On the other hand, asymmetric cryptography relies upon a pair of keys: one public key for encryption purposes and one private key for decryption purposes. This type of cryptography obviates the need for key exchange, yet it does involve a greater degree of computational intensity compared to symmetric cryptography [5-10]. Cryptography as a whole is an ever-evolving field, characterized by ongoing research efforts aimed at developing more robust algorithms and protocols in order to counteract emerging security threats. It serves as the foundational basis for secure communication and the safeguarding of information in the era of digital technology. The majority of people use the internet for transactions, e-mail sharing of important information, online payments, business, video conferencing, online shopping, and other purposes. Security is crucial for all of these uses. Cryptography serves a purpose in security. Cryptography enables us to hoard sensitive information or pass on it over insecure internet networks so that it can only be looked through by the intended recipient [11, 12].

The main purpose of cryptography is to allow two people to communicate over an insecure channel in such a way that the adversary cannot understand what is being said. Encryption is the act of masking data so that it becomes unreadable without special knowledge. This is usually done for confidentiality and usually confidential communication. Encryption is an algorithm that performs encryption (and reverse decryption) in a well-defined series of steps that can be followed as a procedure. The raw data is known as plaintext and the encrypted form is ciphertext. An encrypted text message contains all of the plaintext information but is unreadable by a human or computer without an appropriate decryption mechanism. Encryption is usually parameterized with auxiliary information called a key. Without a key, encryption cannot be used to encrypt or, more importantly, decrypt [13,14].

Recently, researchers have been laboring to shield and preserve data from penetration by attackers. They are finding new approaches of encryption that are sufficient to shield the data of governmental and non-governmental organizations, where encryption takes part an important role in data security and protection [15, 16]. In the field of cryptography, integral transforms have been tried to the exponential functions of prepositions in encoding and decoding operations [17]. In this paper, the Gupta integral transform has been tried in the field of cipher, an approach of writing in which a confidential pattern of a specified set of letters or symbols is employed to represent other letters or symbols, for the encoding of a plain text, and then decoding this cipher for getting the original text.

Some topics in cryptography need to be explained; these notions include [10, 11]:

- Plaintext: the information has to be communicated and it is clear and thorough.
- The term "ciphertext" refers to the processed, unidentifiable form of plaintext that the encryption method would convert over an open, unprotected channel.
- A mathematical approach known as an encryption algorithm is used to produce an encryption key and alter plaintext data such that it becomes unintelligible.

- The decryption algorithm is a mathematical method that employs a decryption key to convert incoming ciphertext into plaintext.
- Cryptography is divided into three branches: symmetric, asymmetric, and protocols. The main difference between these branches is how the cryptographic key is handled. In a symmetric cryptosystem, the key must stay secret and shared between the involved parties only. In asymmetric cryptosystems, two keys are used, private and public. The protocols deal with applications of cryptographic cryptosystems.

The proposed technique uses the symmetric cryptosystem where the key must stay secret and shared between the involved parties only. The key can be transmitted over a secure channel, such as a VPN or SSL/TLS connection, to prevent interception or tampering by malicious parties. For ultimate security, key can be exchanged physically using methods like hand delivery or secure courier services.

The integral Gupta transform has been proposed by the authors Rahul Gupta and Rohit Gupta, and is put into words for a function of exponential order [18]:

Considering functions in the set C, that is $C = \{g(t): \exists\, R, q_1, q_2 > 0,\ |g(t)| < Re^{q_i|(t)|}, if\ t \in (-1)^i X[0,\infty)\}$.

For a given function in set C, the constant R must be a finite number, $q_1\ and\ q_2$, may be finite or infinite.

The integral Gupta transform of a function $g(t)$ is put into words by the integral equations [19]: $\dot{R}\{g(t)\} = G(q) = \frac{1}{q^3}\int_0^\infty e^{-qt}\, g(t)dt, t \geq 0, q_1 \leq q \leq q_2$. The variable q is provided to factor the variable t in the declaration g(t).

The integral Gupta transform of specific functions [20] is given by

1. $\dot{R}\{1\} = \frac{1}{q^3}\int_0^\infty e^{-qy}\, dy = -\frac{1}{q^4}(e^{-\infty} - e^{-0}) = -\frac{1}{q^4}(0-1) = \frac{1}{q^4}$

   Hence $\dot{R}\{1\} = \frac{1}{q^4}$

2. $\dot{R}\{y^n\} = \frac{1}{q^3}\int_0^\infty e^{-qy}\, y^n\, dy = \frac{1}{q^3}\int_0^\infty e^{-z}\left(\frac{z}{q}\right)^n \frac{dz}{q} = \frac{1}{q^{n+4}}\int_0^\infty e^{-z}\,(z)^n dz$

Using the property of gamma function,

$$\dot{R}\{y^n\} = \frac{1}{q^{n+4}}\Gamma(n+1) = \frac{1}{q^{n+4}}n! = \frac{n!}{q^{n+4}}$$

Hence $\dot{R}\{y^n\} = \frac{n!}{q^{n+4}}$

2. Proposed Cryptographic Methodology

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

- ✓ Before starting the encryption process, the sender and receiver must agree on a key called R Key (say).
- ✓ The plain text message is sorted out as a finite chain 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 p = (n+1), then we can form a polynomial g(t) of degree p = (n-1) with an operand considered as a given chain term.
- ✓ Take the integral Gupta transform of a polynomial g(t) found above.
- ✓ Find the ciphertext g_s such that $g_s \equiv p_s \bmod 26$ for all s = 0, 1, 2,…n.
- ✓ The values of g_s for all s (= 0,1,2,….n) will be the encrypted message.

- ✓ Find the key k_s such that $k_s \equiv (p_s - g_s)/26$ $for\ all$ s = 0, 1, 2…n.
- ✓ Thus $p_s = 26k_s + g_s$ *for all* s = 0, 1, 2,…n.
- ✓ The finite sequence that represents the ciphertext is generated.

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

- ✓ Consider the ciphertext and key received from the sender through a secure channel.
- ✓ Convert the given ciphertext to the corresponding finite chain of numbers using the given key k_s for all s = 0, 1, 2,....,n.
- ✓ Finding $p_s = 26k_s + g_s$ for all s =1,2,3,…,(n+1).
- ✓ Taking the inverse Gupta transform of G(q).
- ✓ After converting the numbers in the preceding finite chain to alphabets, the original plain text is obtained.

3. Practical Application of GIT in Cryptography

Here, the practical application of GIT 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.

$$A \equiv 1, B \equiv 2, C \equiv 3, D \equiv 4, \ldots\ldots, Z \equiv 26.$$

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

$$R \equiv 18, E \equiv 5, S \equiv 19, E \equiv 5, A \equiv 1, R \equiv 18, C \equiv 3, H \equiv 8.$$

Here the length of the text i.e. the number of plaintext characters, p = 8. So, the confined series of the text is: (18, 5, 19, 5, 1, 18, 3, 8).

Now, polynomial g(t) of degree n = 7 can be formed with an operand considered as a given chain term and is written as

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

Taking Gupta transform [19] to the above equation, we have

$$G(q) = 18\frac{1}{q^4} + 5\frac{1}{q^5} + 19\left(\frac{2!}{q^6}\right) + 5\,\frac{3!}{q^7} + \frac{4!}{q^8} + 18\,\frac{5!}{q^9} + 3\,\frac{6!}{\mathrm{q10}} + 8\,\frac{7!}{\mathrm{q11}}$$

$$G(q) = \frac{18}{q^4} + \frac{5}{q^5} + \frac{38}{q^6} + \frac{30}{q^7} + \frac{24}{\mathrm{q8}} + \frac{2160}{\mathrm{q9}} + \frac{2160}{\mathrm{q10}} + \frac{6720}{\mathrm{q11}} = \sum_{s=0}^{7} \frac{p_s}{q^{s+4}} \qquad (1)$$

Now finding the ciphertext g_s where $g_s = p_s \bmod 26$ for all s = 0, 1, 2…..7, we have

$g_0 \equiv 18 \bmod 26 = 18.$

$g_1 \equiv 5 \bmod 26 = 5$

$g_2 \equiv 38 \bmod 26 = 12$

$g_3 \equiv 30 \bmod 26 = 4$

$g_4 \equiv 24 \bmod 26 = 24$

$g_5 \equiv 2160 \bmod 26 = 2$

$g_6 \equiv 2160 \bmod 26 = 2$

$g_7 \equiv 6720 \bmod 26 = 12$

Therefore, $p_s = 26k_s + g_s$, for all s = 0, 1, 2,……,7

Here the key 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 fashioned a new confined series as:

$\{g_0, g_1, g_2 \ldots\ldots g_7\} = \{18, 5, 12, 4, 24, 2, 2, 12\}$

This confined series obtained is called ciphertext, which is transcoded to the ciphertext letters "**RELDXBBL**" respectively. This ciphertext will be transmitted to the receiving party over an unsecured channel.

3.2 Decryption (Decoding) Stage

This stage is implemented on the encrypted text to alter it into consistent information.

The encrypted ciphertext and the key are received from the transmitter via a protected route. For instance, the received encrypted text, here is '**RELDXBBL',** and the key is {0, 0, 1, 1, 0, 83, 83, 258}.

The received encrypted text is altered into the equivalent finite chain of the numbers:

$$\{g_0, g_1, g_2 \ldots\ldots g_7\} = \{18, 5, 12, 4, 24, 2, 2, 12\}$$

Since $p_s=26k_s + g_s$ for all s =1,2,3,…,8, therefore, $p_1 = 18$, $p_2 = 5$,$p_3 = 38$,$p_4 = 30$, $p_5 = 24$, $p_6 = 2160$, $p_7 = 2160$, $p_8 = 6720$.

Taking the inverse Gupta transform [20] of G(q) i.e.

$$\dot{R}^{-1}\{G(q)\} = \dot{R}^{-1}\left\{\frac{18}{q^4} + \frac{5}{q^5} + \frac{38}{q^6} + \frac{30}{q^7} + \frac{24}{q8} + \frac{2160}{q9} + \frac{2160}{q10} + \frac{6720}{q11}\right\}$$, we obtain

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

The original plaintext "**RESEARCH**" may be recovered by treating the coefficients of the polynomial g(t) as a finite sequence {18, 5, 19, 5, 1, 18, 3, 8} and then translating the number of the finite sequence to its corresponding alphabet letters, as A=1, B=2, C=3, to Z=26.

4. Discussion

In this paper, the effectiveness and positive result of integral Gupta transform in the field of encryption was demonstrated, because it was used to encrypt plaintext and convert it into encrypted ciphertext, and its inverse showed a positive result to return ciphertext to plaintext. The required plaintext letters are first encoded into their corresponding alphabetic numbers, beginning with A as 1 and ending with Z as 26, as part of the cryptography scheme's proposed encryption algorithm. Next, a series is created that is used in a polynomial with an order n equal to the length of the taken plaintext minus one. The obtained polynomial is transformed using the Gupta transform to produce the ciphertext that is sent across an unprotected channel for the recipient to

receive and decrypt. The key that the recipient will need to decrypt the ciphertext is also the sending party's responsibility. The receiver should receive the produced key via a secure channel. The key can be transmitted over a secure channel, such as a VPN or SSL/TLS connection, to prevent interception or tampering by malicious parties. Moreover, the key can be splitted into multiple parts and each part can be sent separately using different communication channels. This method, known as secret sharing, requires the recipient to combine the parts to reconstruct the original key. In addition, for the ultimate security, key can be exchanged physically using methods like hand delivery or secure courier services. The ciphertext key is generated into a finite series as part of the proposed cryptographic scheme's decryption procedure. The ciphertext original is then recovered from the coefficients of the resulting polynomial by applying the inverse Gupta transform to the finite series.

5. Conclusion

The proposed paper has presented a new cryptographic scheme using integral Gupta transform. The capacity of the Gupta transform to produce a distinct series that differs from other series produced by cryptographic techniques that use other integral transforms is demonstrated by the practical implementation of the suggested cryptographic strategy on an example. Because of this characteristic, the Gupta transform is a useful tool that can be used in the expanding and evolving field of data security as a stand-alone cryptography technique or as a component of more complex techniques. The key of the proposed scheme is the number of multiple of mod n and is extremely difficult for an eyedropper to trace the key by any attack. The proposed technique can be developed and its strength can be increased by utilizing the exponential, trigonometric or logarithmic functions or by combining the integral Gupta transform with other integral transforms available in the literature like Laplace transform, Elzaki transform, Sumudu transform, SEE transform, Aboodh transform, Rohit transform, Dinesh Verma transform, etc.

Acknowledgment

The authors would like to thank Prof. Dinesh Verma for his guidance.

Conflict of Interest

"Conflict of Interest: The authors declare that they have no conflicts of interest."

Funding

There is no financial support in preparation for the publication.

References

1. Kharde U. D., An Application of the Elzaki Transform in Cryptography, *Journal for Advanced Research in Applied Sciences* **2017**, *4*(*5*), 86– 89.
2. Mohammed, N.S. ; Emad, A. Kuffi. Perform the CSI complex Sadik integral transform in cryptography. *Journal of Interdisciplinary Mathematics* **2023** , *26*(*6*),1303–1309.
3. Undegaonkar, H. K.; Ingle, R.N. Role of Some Integral Transforms in Cryptography. *International Journal of Engineering and Advanced Technology* **2020**, *9(3)*, 376-380.
   DOI: https://doi.org/10.35940/ijeat.C5117.029320
4. Kumer P.S.; Vasuki, S.An application of Mahgoub Transform in Cryptography. *Advances in Theoretical and Applied Mathematics* **2018**, *13*(*2*), 91-99.
5. Srinivas,V.; Jayanthi, C.H. Application of the New Integral J-transform in Cryptography. *International Journal of Emerging Technologies* **2020,** *11*(*2*), 678-682.
6. Lakshmi, G. N.; Kumar, B. R., ; Sekhar, A. C.**.** A cryptographic scheme of Laplace transforms, *International Journal of Mathematical Archive* **2011,** *2*(*12*), 2515-2519..
7. Hiwarekar, A.P. A new method of cryptography using Laplace transform, *International Journal of Mathematical Archive* **2012**, *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*. **2022,** *25*(*2*), 35-39.
9. Sedeeg, A. K. H.; Abdelrahim Mahgoub, M. M. ; Saif Saeed, M. A. An Application of the New Integral "Aboodh Transform" in Cryptography, . *Pure and Applied Mathematics Journal*. **2016**,*5* (*5*), 151-154. doi: https://doi.org/10.11648/j.pamj.20160505.12
10. Paar, C.; Pelzl, J. Understanding Cryptography: A Textbook for Students and Practitioners. 2010th Edition Springer-Verlag Berlin Heidelberg. **2010**. https://doi.org/10.1007/978-3-662-69007-9
11. Mansour, E. A.; Kuffi, E. A.; Mehdi, S. A.. Applying SEE Integral Transform in Cryptography. *Samarra Journal of Pure and Applied Science*. **2022**..
12. Menezes, A. J.; Van Oorschot, P. C.; Vanstone, S. A. *Handbook of Applied Cryptography,* CRC Press, 1st edition **1997**. https://doi.org/10.1201/9780429466335
13. Jonathan Katz ; Yehuda Lindell, *Introduction to Modern Cryptography*, Chapman and Hall/CRC, 3rd edition **2021**.
14. Hiwarekar, A.P. New Mathematical Modeling For Cryptography, *Journal of Information Assurance and Security.* **2014**, *9*, 027-033.
15. Akash Thakkar, Ravi Gor, Cryptographic method to enhance the Data Security using RSA algorithm and Sumudu Transform, *Journal of Research in Applied Mathematics. **2023**, 9(4), 48-54.* http://doi.org/10.29121/ijoest.v7.i2.2023.490
16. Jadhav Shaila Shivaji, Hiwarekar A.P., New Method for Cryptography using Laplace-Elzaki Transform, psychology and education **2021**, *58(5)*,1-6
17. Rohit Gupta; Rahul Gupta. Securing data transmission by cryptography using Rohit integral transform. *International Journal Of Engineering & Technology* **2023**,*12*(*2*), 109–11.
18. Rahul Gupta, Rohit Gupta, Dinesh Verma, Propounding a New Integral Transform: Gupta Transform with Applications in Science and Engineering, *International Journal of Scientific Research in Multidisciplinary Studies* **2020**,*6* (*3*), 14-19, March.
19. Rahul Gupta; Rohit Gupta; Rakesh Kumar Verma, Solving Electric Transmission Line Wave Equations via Double Gupta Transform, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)*, **2022**, *11*(*6*), 2533-2538. http://doi.org/10.15662/IJAREEIE.2022.1106029
20. Gupta, R.; Pandita N.; Gupta, R. Solving One-Dimensional Heat and Wave Equations Via Gupta Integral Transform,2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), **2022**, 921-925. https://doi.org/10.1109/ICSCDS53736.2022.9760823