iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 11 **Issue:** VII **Month of publication:** July 2023

**DOI:** https://doi.org/10.22214/ijraset.2023.54750

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue VII Jul 2023- Available at www.ijraset.com*

# Cryptographic Method to Enhance the Data Security using ElGamal Algorithm and Sumudu Transform

Akash Thakkar[1], Ravi Gor[2]
[1]*Research scholar, Department of Applied Mathematical Science, Actuarial Science and Analytics, Gujarat University*
[2]*Department of Applied Mathematical Science, Actuarial Science and Analytics, Gujarat University*

***Abstract:*** ***Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography includes two phases: Encryption and Decryption. Encryption is the process of transforming plaintext to ciphertext, whereas decryption is the reverse procedure. Encryption and decryption schemes based on Sumudu Transform are unable to give more security while communicating the information. ElGamal is a public key algorithm that is based on the discrete logarithm problem. The purpose of this study is to introduce a cryptographic method that uses the ElGamal algorithm and Sumudu Transform to improve communication security.***
***Keywords: Cryptography, Encryption, Decryption, ElGamal, Sumudu Transform.***

## I. INTRODUCTION

Cryptography is a method of protecting data. In cryptography, the procedures used to protect information are based on mathematical principles and a set of rule-based calculations known as algorithms. Cryptography consists of two components: encryption and decryption. Encryption is the process of converting normal data into an unreadable format and decryption is the act of recovering the unreadable data. Cryptography is classified into three types:

*1)* Symmetric key cryptography (secret key cryptography)
*2)* Asymmetric key cryptography (public key cryptography)
*3)* Hash Function

In symmetric key cryptography, the same key is used for encryption and decryption. It is fast and efficient but the drawback is that the sender and receiver must exchange the keys in secure manner. DES, AES, IDEA, RC4, Blowfish, Twofish are some Symmetric key algorithms.

Asymmetric key cryptography also known as public key cryptography that uses two different keys: a public key for encryption and private key for decryption. RSA, DSA, ElGamal, Rabin, ECC are some Asymmetric key algorithms.

### *A. ElGamal Algortihm*

ElGamal algorithm is public key algorithm developed by Taher ElGamal in 1985.
There are mainly three steps in ElGamal algorithm.
(1) Key Generation (2) Encryption process (3) Decryption process

#### *1) Key Generation*

ElGamal involves two keys: public key and private key. Public key is used for encryption and private key is used for decryption of data.

*a)* Select large prime number $p$
*b)* Select primitive element $\alpha \in \mathbb{Z}_p^*$
*c)* Select $K_{pr} = d \in \{2,3,\dots,p-2\}$ as the private key
*d)* Calculate $K_{pub} = \beta = \alpha^d \ mod \ p$ as the public key
*e)* $p, \alpha$ and $\beta$ are published as public key while $d$ should be kept secret as a private key

©IJRASET: All Rights are Reserved 

*2) Encryption process*

*a)* The receiver's public key $(p,\ \alpha,\ \beta)$ is obtained
*b)* Select a random integer number $i$
*c)* Calculate ephemeral key $K_E \equiv \alpha^i \ mod\ p$
*d)* Calculate masking key $K_M \equiv \beta^i \ mod\ p$
*e)* Calculate cipher text as $C \equiv m \cdot K_M \ mod\ p$

Where, $m$ is the secret message which wants to be encrypted

*f)* The cipher text $C$ and $K_E$ sent to the receiver

*3) Decryption Process*

*a)* Calculate masking key $K_M \equiv {K_E}^d \ mod\ p$
*b)* Recover the secret message $m$ by using the formula: $m \equiv C \ \cdot (K_M)^{-1} \ mod\ p$

Some integral transformations contribute to the process of cryptography. Integral transform features are used to create encryption and decryption methods.

### *B. Sumudu Transform (ST)*

Sumudu Transform has very special and useful properties.
Over the set of functions

$$A = \{ f(t) / \exists\ M, \tau_1, \tau_2 > 0\ , |\{f(t)\}| < M\ e^{|t|/\tau_j}, \text{ if } t \in (-1)^j \times [0, \infty)\}$$

Sumudu Transform is defined by

$$G(u) = S[f(t)] = \int_0^\infty e^{-t} f(ut)\ dt = \frac{1}{u}\int_0^\infty e^{\frac{-t}{u}} f(t)\ dt, \qquad u \in (-\tau_1, \tau_2)$$

Sumudu Transform which is itself linear, preserves linear function and hence in particular does not change its unit. Sumudu Transform has many applications in fields such as sciences and engineering.

### *C. Some Standard Functions*

1. Let $f(t) = 1$ then $S[1] = 1$.
2. Let $f(t) = t$ then $S[t] = u$.
3. Let $f(t) = t^2$ then $S[t^2] = 2u^2 = 2!\ u^2$.
4. In general case, if $n > 0$, then $S[t^n] = n!\, u^n$.

### *D. Inverse Sumudu Transform*

1. $S^{-1}[1] = 1$
2. $S^{-1}[u] = t$
3. $S^{-1}[u^2] = \frac{t^2}{2!}$
4. In general case, if $n > 0$, then $S^{-1}[u^n] = \frac{t^n}{n!}$

## II. LITERATURE REVIEW

ElGamal [5] (1985) introduced a method of public key cryptosystem and signature scheme based on discrete logarithms. The security of both systems relies on the difficulty of computing discrete logarithms over finite fields.
Watugala [21] (1993) introduced Sumudu Transform to show interesting properties which makes it easy to visualize. Thus, it is an ideal transform for control engineers and applied mathematicians.
Asiru [9] (2002) discussed the general properties of the Sumudu Transform and some special functions that occur frequently in physical and engineering applications.

Allen [1] (2008) discussed the implementation of several attacks on plain ElGamal encryption and discussed attacks which rely on the underlying mathematics.

Bodkhe and Panchal [2] (2015) introduced a new cryptographic application using Sumudu transform and private key. It is very difficult to find the private key by any other attack. After producing key, they use this key for encryption and decryption that algorithm based on Sumudu transformation and modular arithmetic.

Grewal [6] (2015) discussed ElGamal System which is a public key cryptosystem based on the discrete logarithm problem. He examined its security, advantages, disadvantages and its applications.

Tayal et. al. [14] (2017) provided an overview of network security and various techniques for improving network security. They demonstrated various schemes used in cryptography for network security purposes.

Tuncay [8] (2017) analyzed security based on Sumudu Transform in cryptography and concluded that without knowing the key, the encrypted text can be decrypted.

Dissanayake [4] (2018) studied an improvement of the basic ElGamal public key cryptosystem. The public key of the ElGamal system is not changed in this method. But, the sending structure of message and the decryption process are changed. The ElGamal cryptosystem is not secure under adaptive Chosen Ciphertext Attack (CCA). This improved cryptosystem is immune against Chosen Plaintext Attack (CPA) and Chosen Ciphertext Attack (CCA) attacks. Therefore, this improved system is very suitable for small messages or key exchanges.

Mohammadi et. al. [10] (2018) compared two public key cryptosystems. They focused on the efficient implementation and analysis of the two most popular algorithms for key generation, encryption, and decryption schemes of RSA and ElGamal. RSA is based on the difficulty of prime factorization of a very large number and the ElGamal algorithms hardness is essentially equivalent to the difficulty of finding discrete logarithm modulo a large prime number. These two systems are compared in terms of various parameters such as performance, security and speed. They concluded that RSA is more efficient for encryption than ElGamal and RSA is less efficient for decryption than ElGamal.

Ranasinghe and Athukorala [13] (2020) discussed generalization of the ElGamal public key cryptosystem. They presented a generalization to the original ElGamal system which also relies on the discrete logarithm problem. The encryption process of the scheme is improved such that it depends on the prime factorization of the plaintext. If the plaintext consists of only one distinct prime factor the new method is similar to that of the basic ElGamal algorithm. The proposed system preserves the immunity against the Chosen Plaintext Attack (CPA).

Nagalakshmi et. al. [11] (2020) proposed an implementation of ElGamal scheme for Laplace transform cryptosystem. The time analysis is compared with existing algorithms and comparison reveals that the proposed cryptosystem enhances the data security.

Thakkar and Gor [15] (2021) represented a review of literature concerned with cryptographic algorithms and mathematical transformations. The review of RSA and ElGamal algorithms aids readers in better understanding the differences between the two asymmetric key cryptographic algorithms and how they work and review of mathematical transformations helps the reader to understand how mathematical transformations are used in cryptography.

Thakkar and Gor [16] (2022) developed a cryptographic method using RSA algorithm and Kamal Transform to improve security of communication. This paper provided frequency test and statistical analysis on the proposed method.

Thakkar and Gor [17] (2022) developed a cryptographic method using ElGamal algorithm and Kamal Transform to improve security of communication. The frequency test and statistical analysis on the proposed method are provided in this work.

Thakkar and Gor [18] (2022) developed a cryptographic method using the ElGamal algorithm and Mellin Transform to improve security of communication. The frequency test and statistical analysis on the proposed method are provided in this work.

Thakkar and Gor [19] (2023) developed a cryptographic method using RSA algorithm and Mellin Transform to improve security of communication. This paper provided frequency test and statistical analysis on the proposed method.

Thakkar and Gor [20] (2023) developed a cryptographic method using the RSA algorithm and Sumudu Transform to improve security of communication. The frequency test and statistical analysis on the proposed method are provided in this work.

## III. PROPOSED ALGORITHM OF THE MATHEMATICAL MODEL

The proposed method is ElGamal algorithm with application of Sumudu Transform (ElGamal-ST). The proposed work is to improve security of communication. When two people want to transfer the data, they will follow the given steps for encryption and decryption.

The following method provides an overview of the proposed cryptographic scheme.

*1) Method of Key Generation*

Following are the steps involved in Key Generation.

Step 1: Generate large prime number $p$

Step 2: Select primitive element $\alpha \in \mathbb{Z}_p^*$

Step 3: Select $K_{pr} = d \in \{2,3,\dots,p-2\}$

Step 4: Calculate $K_{pub} = \beta = \alpha^d \ mod \ p$

Step 5: Generate polynomial $p(t)$ using primitive element $\alpha$. i.e., $p(t) = \sum_{i=0}^{m} \alpha^{i+3} \ t^{i+3}$

*2) Method of Encryption*

Following are the steps involved in Encryption.

Step 1: Select the plain text $P_0, P_1, \dots, P_m$, convert into ASCII code integer $M_0, M_1, \dots, M_m$

Step 2: Calculate $M_i(p(t)) = M_i \sum_{i=0}^{m} \alpha^{i+3} \ t^{i+3} = \sum_{i=0}^{m} G_i \ t^{i+3}$

Step 3: Apply Sumudu Transform of a polynomial, i.e., $S\left[\sum_{i=0}^{m} G_i \ t^{i+3}\right] = \sum_{i=0}^{m} R_i \ u^{i+3}$

Step 4: Find $r_i$ such that $r_i \equiv R_i \ mod \ p$

Step 5: Find $k_i$ such that $k_i = (R_i - r_i)/p$

Step 6: Select $l \in \{2,3,\dots,p-2\}$

Step 7: Calculate ephemeral key $K_E \equiv \alpha^l \ mod \ p$

Step 8: Calculate masking key $K_M \equiv \beta^l \ mod \ p$

Step 9: Calculate $C_i \equiv R_i \cdot K_M \ mod \ p$ then get integer of cipher text $C_0, C_1, \dots, C_m$

Step 10: Each integer of cipher text $C_0, C_1, \dots, C_m$ is converted to its construct by ASCII character are stored as the cipher text $C$

*3) Method of Decryption*

Following are the steps involved in Decryption.

Step 1: Consider the Cipher text and key received from the sender

Step 2: Cipher text $C$ converted to ASCII values of $C_0, C_1, \dots, C_m$

Step 3: Calculate masking key $K_M \equiv {K_E}^d \ mod \ p$

Step 4: Each integer of $C_0, C_1, \dots, C_m$ is converted into $m_i \equiv C_i \cdot (K_M)^{-1} \ mod \ p$ and get $m_0, m_1, \dots, m_m$

Step 5: Calculate $R_i = m_i + (p \cdot k_i)$ and get $R_0, R_1, \dots, R_m$

Step 6: Find the polynomial assuming $R_i$ as a coefficient

Step 7: Apply inverse Sumudu transform, i.e., $S^{-1}\left[\sum_{i=0}^{m} R_i \ u^{i+3}\right] = \sum_{i=0}^{m} G_i \ t^{i+3}$
and find $M_i$ as $\frac{G_i}{\alpha^{i+3}}$

Step 8: Each integer $M_i$ are converted to their corresponding ASCII code values and hence get the original plain text $P_0, P_1, \dots, P_m$

Public key: $\{p, \alpha, \beta, p(t), k_i, K_E\}$

Private key: $\{d\}$

## IV. NUMERICAL EXAMPLE

This section contains an example of an encryption and decryption method. Note that, the parameters are chosen to make computation easier, however they are not in the useable range for secure transmission.

If Alice (sender) wants to send an encrypted message to Bob (receiver).

Bob first computes his parameters using steps as given in method of Key Generation.

*1)* Step 1: Prime number $p = 131$

*2)* Step 2: Primitive element $\alpha = 29$

*3)* Step 3: $K_{pr} = d = 63$

*4)* Step 4: $K_{pub} = \beta = \alpha^d \ mod \ p = 29^{63} \ mod \ 131 = 50$

*5)* Step 5: Polynomial $p(t)$ using primitive element $\alpha = 29$
i.e., $p(t) = \sum_{i=0}^{m} 29^{i+3} \ t^{i+3}$

Bob then sends his public key $(p, \alpha, \beta, p(t))$ to Alice.

Alice computes his parameters to encrypt the message using steps as given in method of Encryption.

- Step 1: Plain text = " CryPto ", $P_0 = C, P_1 = r, P_2 = y, P_3 = P, P_4 = t, P_5 = o$,
  convert into ASCII code integer $M_0 = 67, M_1 = 114, M_2 = 121, M_3 = 80, M_4 = 116, M_5 = 111$
- Step 2: $M_i(p(t)) = \sum_{i=0}^{5} M_i\, 29^{i+3}\, t^{i+3}$
  $= 1634063 \cdot t^3 + 80630034 \cdot t^4 + 2481849029 \cdot t^5 + 47585865680 \cdot t^6$
  $+2000985651844 \cdot t^7 + 55527351838671 \cdot t^8$
  $= \sum_{i=0}^{5} G_i\, t^{i+3}$
- Step 3: $S\left[\sum_{i=0}^{5} G_i\, t^{i+3}\right] = S\,[1634063 \cdot t^3 + 80630034 \cdot t^4 + 2481849029 \cdot t^5 + 47585865680 \cdot t^6$
  $+2000985651844 \cdot t^7 + 55527351838671 \cdot t^8]$
  $= 3! \cdot 1634063 \cdot u^3 + 4! \cdot 80630034 \cdot u^4 + 5! \cdot 2481849029 \cdot u^5$
  $+6! \cdot 47585865680 \cdot u^6 + 7! \cdot 2000985651844 \cdot u^7 + 8! \cdot 55527351838671 \cdot u^8$
  $= 9804378 \cdot u^3 + 1935120816 \cdot u^4 + 297821883480 \cdot u^5$
  $+34261823289600 \cdot u^6 + 10084967685293760 \cdot u^7 + 2238862826135214720 \cdot u^8$
  $= \sum_{i=0}^{5} R_i\, u^{i+3}$
  we get, $R_0 = 9804378, R_1 = 1935120816, R_2 = 297821883480, R_3 = 34261823289600,$
  $R_4 = 10084967685293760, R_5 = 2238862826135214720$
- Step 4: Find $r_i$ such that $r_i \equiv R_i \bmod 131$,
  we get, $r_0 = 76, r_1 = 82, r_2 = 28, r_3 = 62, r_4 = 80, r_5 = 75$
- Step 5: Find $k_i$ such that $k_i = (R_i - r_i)/131$,
  we get, $k_0 = 74842, k_1 = 14771914, k_2 = 2273449492, k_3 = 261540635798,$
  $k_4 = 76984486147280, k_5 = 17090555924696295$
- Step 6: Select $l = 79$
- Step 7: Calculate ephemeral key $K_E \equiv \alpha^l \bmod p \equiv 29^{79} \bmod 131 = 66$
- Step 8: Calculate masking key $K_M \equiv \beta^l \bmod p \equiv 50^{79} \bmod 131 = 127$
- Step 9: Calculate cipher text $C_i \equiv R_i \cdot K_M \bmod 131$
  we get, $C_0 = 89, C_1 = 65, C_2 = 19, C_3 = 14, C_4 = 73, C_5 = 35$
- Step 10: Each integer of cipher text $C_0 = 89, C_1 = 65, C_2 = 19, C_3 = 14, C_4 = 73, C_5 = 35$ is converted to its construct by ASCII character $C_0 = Y, C_1 = A, C_2 = DC3, C_3 = SO, C_4 = I, C_5 = \#$ and stored as the cipher text $C =$ "***YADC3SOI#***"

Alice then sends ($k_i$, $K_E$, cipher text $C$) to Bob.

Bob decrypts the cipher text using steps as given in method of Decryption.

- Step 1: Consider the Cipher text and key received from the sender.
- Step 2: The cipher text $C =$ "$YADC3SOI\#$ "converted to ASCII values of
  $C_0 = 89, C_1 = 65, C_2 = 19, C_3 = 14, C_4 = 73, C_5 = 35$
- Step 3: Calculate masking key $K_M \equiv K_E{}^d \bmod p \equiv 66^{63} \bmod 131 = 127$
- Step 4: Each integer of $C_0 = 89, C_1 = 65, C_2 = 19, C_3 = 14, C_4 = 73, C_5 = 35$ is converted into
  $m_i \equiv C_i \cdot (K_M)^{-1} \bmod p$
  we get, $m_0 = 76, m_1 = 82, m_2 = 28, m_3 = 62, m_4 = 80, m_5 = 75$
- Step 5: Calculate $R_i = m_i + (p \cdot k_i)$
  we have, $k_0 = 74842, k_1 = 14771914, k_2 = 2273449492, k_3 = 261540635798,$
  $k_4 = 76984486147280, k_5 = 17090555924696295$
  we get, $R_0 = 9804378, R_1 = 1935120816, R_2 = 297821883480, R_3 = 34261823289600,$
  $R_4 = 10084967685293760, R_5 = 2238862826135214720$
- Step 6: The polynomial assuming $R_0 = 9804378, R_1 = 1935120816, R_2 = 297821883480,$
  $R_3 = 34261823289600, R_4 = 10084967685293760, R_5 = 2238862826135214720$ as a coefficient
  $9804378 \cdot u^3 + 1935120816 \cdot u^4 + 297821883480 \cdot u^5 + 34261823289600 \cdot u^6 +$
  $10084967685293760 \cdot u^7 + 2238862826135214720 \cdot u^8$

- Step 7: Apply inverse Sumudu transform,

$$S^{-1}[\sum_{i=0}^{5} R_i\, u^{i+3}] = S^{-1}[9804378 \cdot u^3 + 1935120816 \cdot u^4 + 297821883480 \cdot u^5 + 34261823289600 \cdot u^6 + 10084967685293760 \cdot u^7 + 2238862826135214720 \cdot u^8]$$

$$= \frac{9804378 \cdot t^3}{3!} + \frac{1935120816 \cdot t^4}{4!} + \frac{297821883480 \cdot t^5}{5!} + \frac{34261823289600 \cdot t^6}{6!} + \frac{10084967685293760 \cdot t^7}{7!} + \frac{(2238862826135214720 \cdot t^8)}{8!}$$

$$= 1634063 \cdot t^3 + 80630034 \cdot t^4 + 2481849029 \cdot t^5 + 47585865680 \cdot t^6 + 2000985651844 \cdot t^7 + 55527351838671 \cdot t^8$$

$$= \sum_{i=0}^{5} G_i\, t^{i+3}$$

Compute $\frac{G_i}{\alpha^{i+3}}$ and get integer $M_0, M_1, \dots, M_5$

we get, $M_0 = 67, M_1 = 114, M_2 = 121, M_3 = 80, M_4 = 116, M_5 = 111$

- Step 8: Each integer $M_0 = 67, M_1 = 114, M_2 = 121, M_3 = 80, M_4 = 116, M_5 = 111$ are converted to them corresponding ASCII code values $P_0 = C, P_1 = r, P_2 = y, P_3 = P, P_4 = t, P_5 = o$ and hence get the original plain text = " **CryPto** "

## V. TESTING AND ANALYSIS

The statistical analysis and frequency testing for this proposed method are presented. The graph of frequency distribution for ElGamal algorithm and proposed method ElGamal-ST is shown here and also compared with each other. We used ElGamal, ST and proposed method ElGamal-ST of correlation coefficients in statistical analysis.

### *A. Frequency Test*

Figure I show that the frequency of the same character in plaintext after encryption with ElGamal algorithm is the same, where the x-axis and y-axis represent plaintext and frequency level of ciphertext values, respectively.

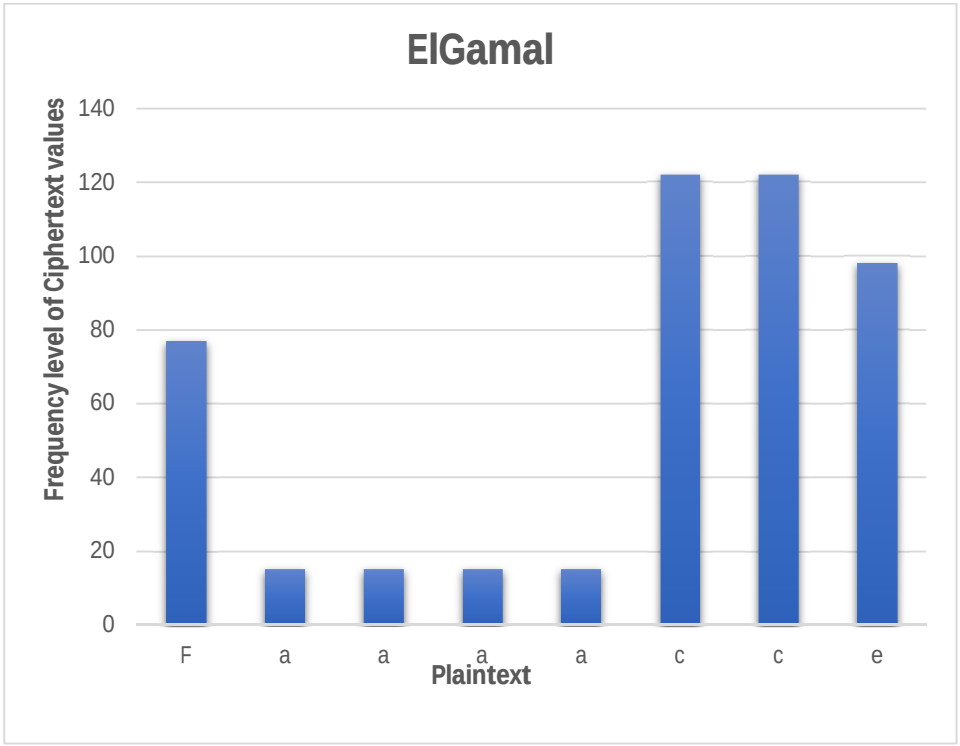



Fig. I: ElGamal algorithm ciphertext frequency distribution

Figure II show that the frequency of each character in a plaintext has different frequency after encryption with the proposed method ElGamal-ST, where plaintext and frequency level of ciphertext values are considered on x-axis and y-axis respectively.

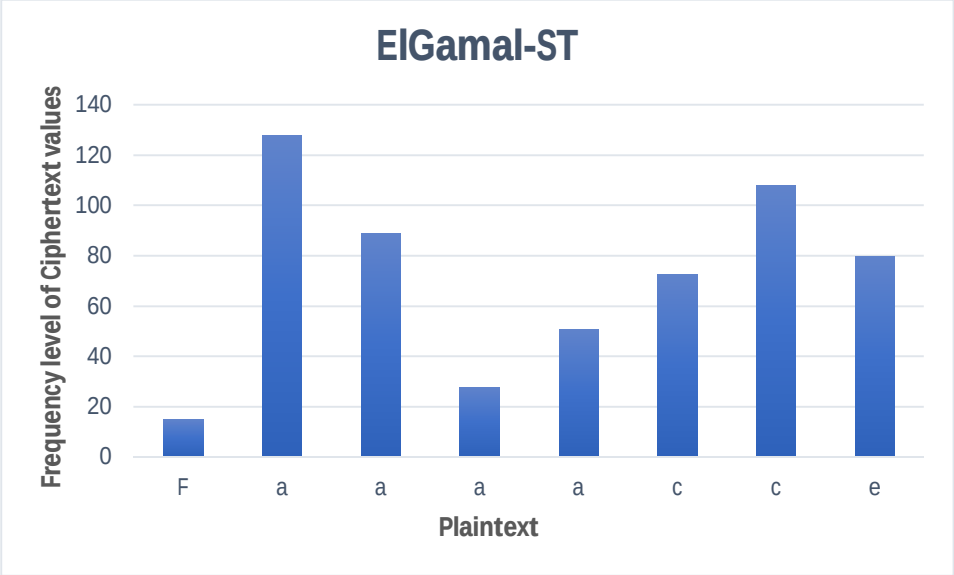



Fig. II: The proposed algorithm ciphertext frequency distribution

Figure III show that graphical representation of the frequency distribution for ElGamal algorithm and proposed method ElGamal-ST.

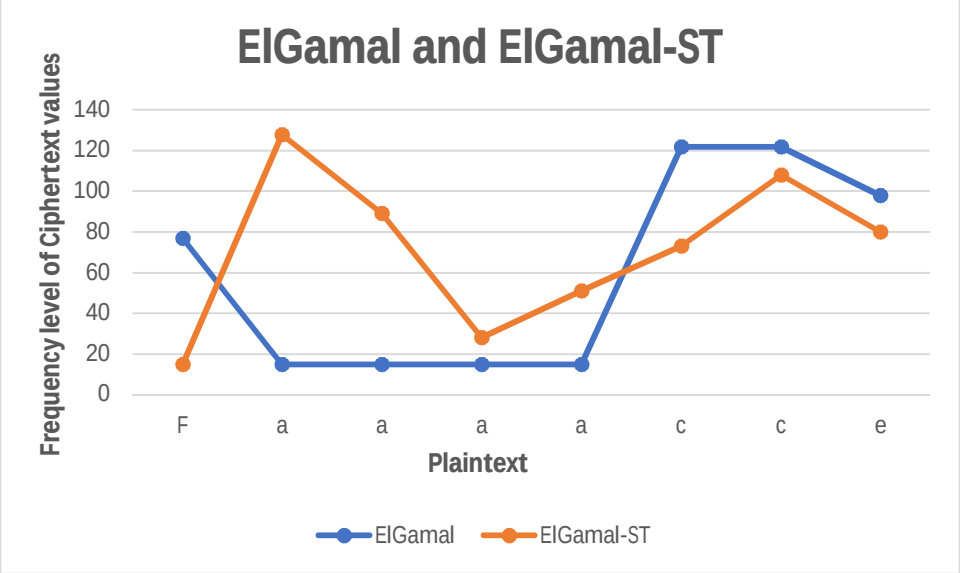



Fig. III: Ciphertext frequency distribution of ElGamal and ElGamal-ST

According to the frequency test, the proposed method ElGamal-ST has a different frequency for each repeated character in a plaintext after encryption.

*B. Statistical Analysis*

In statistics, correlation coefficients are used to assess how closely two variables are related. The aim of the proposed method of research is to examine and create an algorithm that strongly resists cryptographic attacks. The correlation coefficient between the values of plaintext and ciphertext are examined. Plaintext and ciphertext are identical if the correlation coefficient is one. Plaintext and ciphertext are completely different if the correlation coefficient is near to zero. If the correlation coefficient is less than one, ciphertext is the inverse of plaintext. As a result, encryption success is associated with lower correlation coefficient values. Table shows the experimental finding of the correlation coefficient values for ElGamal algorithm, ST method and proposed method ElGamal-ST.

Table: The Correlation test from plaintext to ciphertext values

| Message | Method | Correlation |
|---|---|---|
| Applied | ElGamal algorithm | 0.13466092 |
| | ST method | 0.71115463 |
| | ElGamal-ST proposed method | 0.08925833 |
| CryPto | ElGamal algorithm | -0.79330274 |
| | ST method | -0.82827718 |
| | ElGamal-ST proposed method | -0.2318453 |
| SYSTEM | ElGamal algorithm | -1 |
| | ST method | -0.67114024 |
| | ElGamal-ST proposed method | 0.47049216 |
| Ac@demic | ElGamal algorithm | 0.89970967 |
| | ST method | -0.44955655 |
| | ElGamal-ST proposed method | -0.203351 |

According to the correlation test, proposed method ElGamal-ST gives better result compare to ElGamal or ST. Correlation coefficient values are closer to zero with this proposed method ElGamal-ST. However, for some data (message), ElGamal may perform better than ElGamal-ST. Such cases and conditions under which the performance can be generalized is a direction for further research.

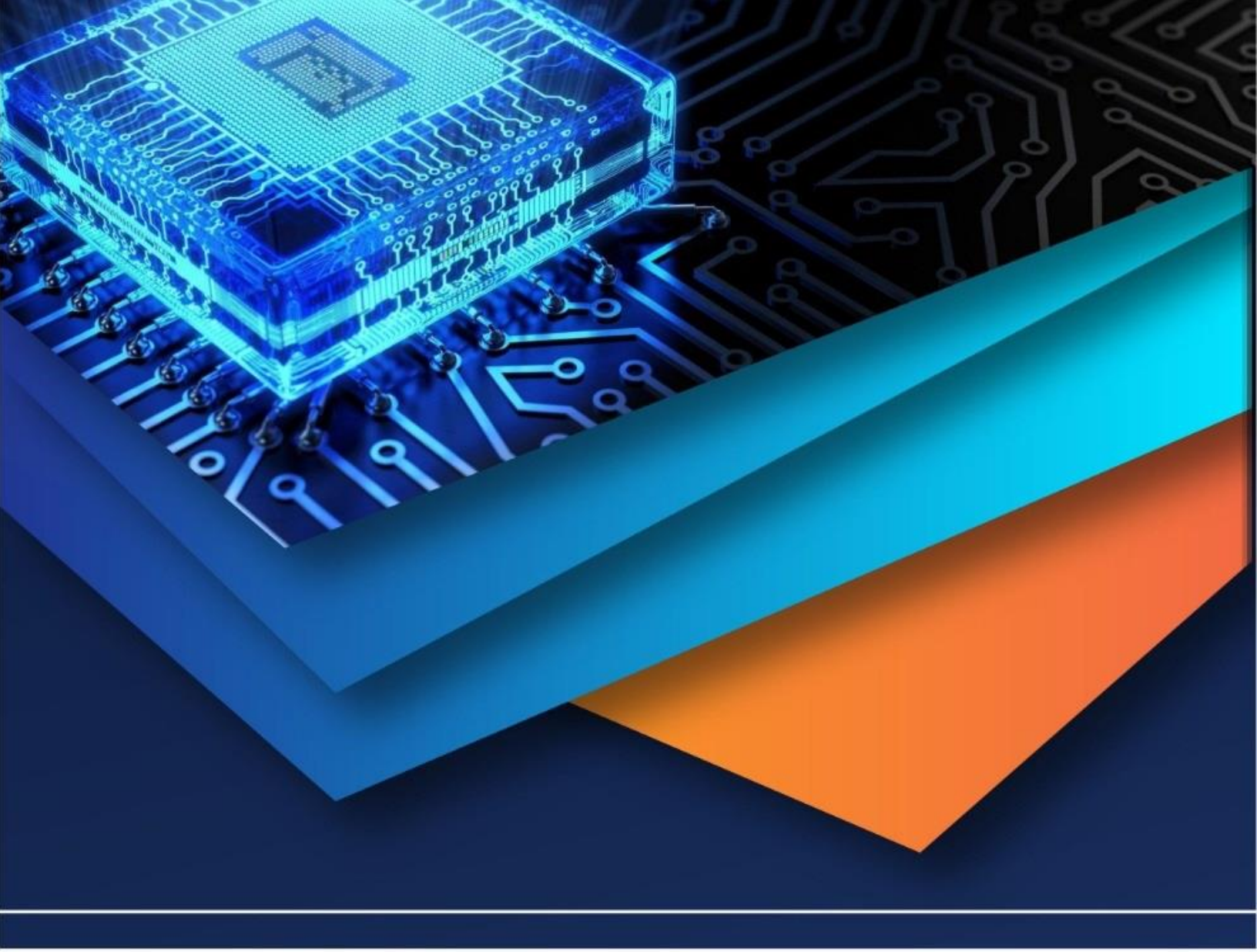
## VI. CONCLUSION

Cryptography is one of the most important fundamental tools to provide security to data communication. An application of Sumudu Transform for cryptographic process is a weak scheme because encrypted data can be decrypted by elementary modular arithmetic. ElGamal is a widely used public key cryptosystem that is based on the difficulty of computing discrete logarithms over finite fields. The proposed work expands on innovative method using ElGamal algorithm with application of Sumudu Transform. It is impossible to break this method without knowing the private key. Therefore, this proposed method ElGamal-ST can provide more security of communication.

## REFERENCES

[1] Allen B. (2008). “Implementing several attacks on plain ElGamal encryption”, Iowa State University.
[2] Bodkhe D. S, Panchal S. K. (2015). “Use of Sumudu Transform in Cryptography”, Bulletin of the Marathwada Mathematical society, 16/2: 1-6.
[3] Debnath L. and Bhatta D. (2015). “Integral Transforms and Their Applications” (Third Edition), 978-1-4822-2358-3.
[4] Dissanayake W. D. M. G. M. (2018). “An Improvement of the Basic El-Gamal Public Key Cryptosystem”, International Journal of Computer Applications Technology and Research, 7(2), 40-44.
[5] ElGamal T. (1985). “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE transactions on information theory, 31(4), 469-472.
[6] Grewal J. (2015). “ElGamal: Public-Key Cryptosystem”, Math and Computer Science Department, Indiana State University.
[7] Jeevitha S., Komala S., Silambarasi S., Susitha S.,Vanitha R. (2021). “An introduction of sumudu transform”, Journal of Emerging Technologies and Innovative Research (JETIR), Volume 8, Issue 7, JETIR2107602, (ISSN-2349-5162).
[8] M. Tuncay GENÇOĞLU (2017). “Cryptanalysis Use of Sumudu Transform in Cryptography”, researchgate/publication/319213093.
[9] Muniru Aderemi Asiru, “Further properties of the Sumudu transform and its applications”, International Journal of Mathematical Education in Science and Technology 33 (2002).
[10] Mohammadi M., Zolghadr A., Purmina M. A. (2018). “Comparison of two Public Key Cryptosystems”, Journal of Optoelectronical Nanostructures Summer, 3(3), 47-58.
[11] Nagalakshmi G., Sekhar A. C., Sankar N. R. (2020). “An Implementation of ElGamal Scheme for Laplace Transform Cryptosystem”, International Journal of Computer Science and Engineering (IJCSE), ISSN: 2231-3850, 11(1).
[12] Paar C. and Pelzl J. (2009). “Understanding cryptography: a textbook for students and practitioners”, Springer Science & Business Media.
[13] Ranasinghe R. and Athukorala P. (2020). “A Generalization of the ElGamal public-key cryptosystem”, IACR Cryptol. ePrint Arch., 2020, 354.
[14] Tayal S., Gupta N., Gupta P., Goyal D., Goyal M. (2017). “A review paper on network security and cryptography”, Advances in Computational Sciences and Technology, 10(5), 763-770.
[15] Thakkar A. and Gor R. (2021). “A Review paper on Cryptographic Algorithms and Mathematical Transformations”, Proceeding of International Conference on Mathematical Modelling and Simulation in Physical Sciences (MMSPS), Excellent Publishers, ISBN: 978-81-928100-1-0, 324-331.
[16] Thakkar A. and Gor R. (2022). “Cryptographic method to enhance the Data Security using RSA algorithm and Kamal Transform”, IOSR Journal of Computer Engineering (IOSR-JCE), 24(3), 2022, pp. 01-07.

[17] Thakkar A. and Gor R. (2022). "Cryptographic method to enhance the Data Security using ElGamal algorithm and Kamal Transform", IOSR Journal of Computer Engineering (IOSR-JCE), 24(3), 2022, pp. 08-14.
[18] Thakkar A. and Gor R. (2022), "Cryptographic method to enhance Data Security using ElGamal algorithm and Mellin Transform", IOSR Journal of Mathematics (IOSR-JM), 18(6), (2022), pp. 12-18.
[19] Thakkar A. and Gor R. (2023), "Cryptographic Method to Enhance Data Security Using RSA Algorithm and Mellin Transform", International Journal of Engineering Science Technologies (IJOEST), 7(2), pp. 63-72.
[20] Thakkar A. and Gor R. (2023), "Cryptographic method to enhance Data Security using RSA algorithm and Sumudu Transform", Quest Journal of Research in Applied Mathematics, 9(4), pp. 48-54.
[21] Watugala G. K.: Sumudu Transform – "An Integral transform to solve differential equations and control engineering problems", International Journal of Mathematical Education in Science and Technology, 24(1), 35 - 43, (1993).
[22] William Stallings. "Cryptography and Network Security", ISBN 81-7758-011-6, Pearson Education, Third Edition.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)