IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 18, Issue 6 Ser. II (Nov. – Dec. 2022), PP 12-18
www.iosrjournals.org

Cryptographic method to enhanceData Security using ElGamal algorithm and Mellin 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*
[1]*akashthakkar@gujaratuniversity.ac.in*

Abstract:*Cryptography is a popular technique for ensuring information confidentiality.Cryptography is divided into two stages: encryption and decryption.Encryption is the process of transforming plaintext to ciphertext, whereas decryption is the reverse procedure.Encryption and decryption schemes based on Mellin Transformation 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 Mellin Transform to improve communication security.*

Keywords:*Plaintext, Ciphertext, Encryption, Decryption, ElGamal algorithm, Mellin Transform.*

Date of Submission: 15-11-2022 Date of Acceptance: 01-12-2022

I. INTRODUCTION

Cryptography is a widely used approach for information security.Encryption and decryption are two basic cryptographic functions.Encryption is the process of transforming normal data into an unreadable form, whereas decryption is the act of recovering the unreadable data.Cryptography is classified into three types:

- Symmetric key cryptography (secret key cryptography)
- Asymmetric key cryptography (public key cryptography)
- Hash Function

Symmetric key cryptography is an encryption technique in which the same key is used to encrypt and decrypt data. Symmetric key cryptography is fast and easy, the disadvantage is that the transmitter and receiver must exchange keys in a secure manner. DES, AES, IDEA, RC4, Blowfish, Twofish are some Symmetric key algorithms.

Asymmetric key cryptography,often known as public-key cryptography, is a procedure that encrypts and decrypts data using a pair of related keys - one public key and one private key.RSA, DSA, ElGamal, Rabin, ECC are some Asymmetric key algorithms.

A. ElGamal Algorithm

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 algorithm(3) Decryption algorithm

(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, α and β are published as public key while d should be kept secret as a private key

(2) Encryption algorithm

a) The receiver's public key (p, α, β) 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 algorithm

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. Mellin Transform (MT)

TheMellin Transform is an integral Transform named after the finnish mathematician Hjalmar Mellin (1854-1933). The Mellin Transform is extremely useful for certain applications including solving Laplace equations.
Let $F(x)$ a function defined for all positive values of t, then the Mellin Transform of $f(x)$ is defined by

$$f(x)^*(s) = \int_0^\infty f(x)x^{s-1}\ dx$$

Properties of Mellin Transform:

1. Scaling: $f^*(at)(s) = a^{-s}f^*(s)$.
2. Inverse of independent variable: $(x^{-1}\ f(x^{-1}))^* = f^*(1-s)$.
3. Multiplication by Power of $ln\ x$: $((\ln x)^k\ (f(x)))^* = \frac{d^k}{ds^k}\ f*(s)$.
4. Derivative: $(\frac{d^k}{dx^k}\ f(x))^* = (-1)^k(s-k)_k f^*(s-k)$.
   Where: $(s-k)_k = (s-k)(s-j+1)\ldots(s-1) = \frac{\Gamma(s)}{\Gamma(s-k)}$.
5. Convolution: $(f(x)g(x))^* = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(z)G(s-z)dz$.

II. LITERATURE REVIEW

ElGamal[4](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.

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

Santana[12](2014) developed a scheme in cryptography whose construction is based on the application of Mellin Transform.

Dissanayake[3] (2015) 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.

Grewal [5](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 on Network Security and various techniques through which Network Security can be enhanced i.e., Cryptography. They displayed different plans which are utilized as a part of cryptography for Network security reason.

Mohammadi et. al.[8] (2018) compared two public key cryptosystems. They focused on efficient implementation and analysis of two most popular of these algorithms, RSA and ElGamal for key generation, encryption and decryption schemes. RSA relies on the difficulty of prime factorization of a very large number and the hardness of ElGamal algorithm is essentially equivalent to the hardness of finding discrete logarithm modulo a large prime number. These two systems are compared to each other from points of view of different parameters such as performance, security, speed and applications. They concluded that RSA is more efficient for encryption than ElGamal and RSA is less efficient for decryption than ElGamal.

Johar[6](2019) presented basic introduction of Mellin Transform and its examples.

Ranasinghe and Athukorala[11](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. [9](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.

III. PROPOSED ALGORITHM OF THE MATHEMATICAL MODEL

The proposed method is ElGamal algorithm with application of Mellin Transform (ElGamal-MT). The proposed work is to improve security of communication. When two party want to transfer the data, they will follow the given steps for encryption and decryption. The following method provides an insight into the proposed cryptographic scheme.

A. Method of Key Generation

Steps involved in Key Generation as follows.

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 $p(x)$ using primitive element α.i.e., $p(x) = \sum_{i=1}^{m} \alpha^i x^i$

B. Method of Encryption

Steps involved in Encryption as follows.

Step 1: Select the plain text $P_1, P_2, \dots, P_m$, convert into ASCII code integer $M_1, M_2, \dots, M_m$

Step 2: Calculate $\sum_{i=1}^{m} M_i(p(x))$

Step 3: Generating function $L(x) = \sum_{i=1}^{m} e^{-x}(M_i(p(x))$ from that we get $\sum_{i=1}^{m} G_i$

Step 4: Take Mellin Transform of a function.i.e., $L(x)^* = \sum_{i=1}^{m} G_i(s+i-1)! = \sum_{i=1}^{m} R_i$

Step 5: Choose s and get$\sum_{i=1}^{m} R_i$

Step 6: Find r_i such that $r_i \equiv R_i \ mod \ p$

Step 7: Find k_i such that $k_i = (R_i - r_i)/p$

Step 8: Select $l \in \{2,3, \dots, p-2\}$

Step 9: Calculate ephemeral key $K_E \equiv \alpha^l \ mod \ p$

Step 10: Calculate masking key $K_M \equiv \beta^l \ mod \ p$

Step 11: Calculate $C_i \equiv R_i \cdot K_M \ mod \ p$then get integer of cipher text $C_1, C_2, \dots, C_m$

Step 12: Each integer of cipher text $C_1, C_2, \dots, C_m$ is converted to its construct by ASCII characterare stored as the cipher text C

C. Method of Decryption

Steps involved in Decryption as follows.

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

Step 2: Cipher text C converted to ASCII values of $C_1, C_2, \dots, C_m$

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

Step 4: Each integer of $C_1, C_2, \dots, C_m$ is converted into $m_i \equiv C_i \cdot (K_M)^{-1} \ mod \ p$and get $m_1, m_2, \dots, m_m$
Step 5: Calculate $R_i = m_i + (p * k_i)$ and get $R_1, R_2, \dots, R_m$
Step 6: Find the polynomial assuming R_i as a coefficient
Step 7: Apply inverse Mellin Transform. i.e., $L^*(x) = e^{-x} \sum_{i=1}^{m} R_i \, x^i$and get integer $M_1, M_2, \dots, M_m$
Step 8: Each integer M_i are converted to their corresponding ASCII code values and hence getthe original plain text $P_1, P_2, \dots, P_m$

Public key: $\{p, \alpha, \beta, p(x), k_i, K_E\}$
Private key: $\{d\}$

IV. NUMERICAL EXAMPLE

In this section we present the example for method of Encryption and Decryption. 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.
Step 1: Prime number $p = 67$
Step 2: Primitive element $\alpha = 18$
Step 3:$K_{pr} = d = 12$
Step 4:$K_{pub} = \beta = \alpha^d \ mod \ p = 18^{12} \ mod \ 67 = 14$
Step 5: Polynomial $p(x)$ using primitive element $\alpha = 18$
i.e., $p(x) = \sum_{i=1}^{m} 18^i t^i$

Bob then sends his public key $(p, \alpha, \beta, p(x))$ to Alice.
Alice computes his parameters to encrypt the message using steps as given in method of Encryption.
Step 1: Plain text = "**M@th**", $P_1 = M, P_2 = @, P_3 = t, P_4 = h$,convert into ASCII code integer
$M_1 = 77, M_2 = 64, M_3 = 116, M_4 = 104$
Step 2: $\sum_{i=1}^{4} M_i\big(p(x)\big) = \sum_{i=1}^{4} M_i(\ 18^i x^i)$
$= 1386 \cdot x + 20736 \cdot x^2 + 676512 \cdot x^3 + 10917504 \cdot x^4$
Step 3: $L(x) = \sum_{i=1}^{4} e^{-x}[M_i(18^i x^i)]$
$= e^{-x}\ [1386 \cdot x + 20736 \cdot x^2 + 676512 \cdot x^3 + 10917504 \cdot x^4]$
we get, $G_1 = 1386, G_2 = 20736, G_3 = 676512, G_4 = 10917504$
Step 4: Take Mellin Transform of a function.i.e., $L(x)^* = \sum_{i=1}^{m} G_i(s + i - 1)! = \sum_{i=1}^{m} R_i$
Step 5: Choose $s = 3$ and
we get, $R_1 = 8316, R_2 = 497664, R_3 = 81181440, R_4 = 7860602880$
Step 6: Find r_i such that $r_i \equiv R_i \ mod \ 67$,
we get, $r_1 = 8, r_2 = 55, r_3 = 19, r_4 = 3$
Step 7: Find k_i such that $k_i = (R_i - r_i)/67$ and $k_0 = 3$ (value of s)
we get, $k_1 = 124, k_2 = 7427, k_3 = 1211663, k_4 = 117322431$
Step 8: Select $l = 21$
Step 9: Calculate ephemeral key $K_E \equiv \alpha^l \ mod \ p \equiv 18^{21} \ mod \ 67 = 43$
Step 10: Calculate masking key $K_M \equiv \beta^l \ mod \ p \equiv 14^{21} \ mod \ 67 = 24$
Step 11: Calculate cipher text $C_i \equiv R_i \cdot K_M \ mod \ 67$
we get, $C_1 = 58, C_2 = 47, C_3 = 54, C_4 = 5$
Step 12: Each integer of cipher text $C_1 = 58, C_2 = 47, C_3 = 54, C_4 = 5$ is converted to itsconstruct by ASCII character$C_1 = :, C_2 = /, C_3 = 6, C_4 =$\x05 and stored as thecipher text $C =$ ":/**6\x05**"

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: Cipher text $C =$ " :/**6\x05**" converted to ASCII values of$C_1 = 58, C_2 = 47, C_3 = 54, C_4 = 5$
Step 3: Calculate masking key $K_M \equiv {K_E}^d \ mod \ p \ \equiv 43^{12} \ mod \ 67 = 24$
Step 4: Each integer of $C_1 = 58, C_2 = 47, C_3 = 54, C_4 = 5$is converted into$m_i \equiv C_i \cdot (K_M)^{-1} \ mod \ p$
we get,$m_1 = 8, m_2 = 55, m_3 = 19, m_4 = 3$

Step 5: Calculate $R_i = m_i + (p * k_i)$ and
we have, $k_1 = 124, k_2 = 7427, k_3 = 1211663, k_4 = 117322431$
we get,$R_1 = 8316, R_2 = 497664, R_3 = 81181440, R_4 = 7860602880$
Step6: The polynomial assuming $R_1 = 8316, R_2 = 497664, R_3 = 81181440, R_4 = 7860602880$ as a coefficient$8316 * x + 497664 * x^2 + 81181440 * x^3 + 7860602880 * x^4$
Step 7: Apply inverse Mellin Transform

$$L^*(x) = e^{-x} \sum_{i=1}^{4} R_i x^i$$

$$= e^{-x}[8316 * x + 497664 * x^2 + 81181440 * x^3 + 7860602880 * x^4]$$

and get $\sum_{i=1}^{4} G_i = \sum_{i=1}^{4} \frac{R_i}{(s+i-1)!}$and we have $k_0 = 3$ (as value of s)
From G_i get integer $M_1 = 77, M_2 = 64, M_3 = 116, M_4 = 104$
Step 8: Each integer $M_1 = 77, M_2 = 64, M_3 = 116, M_4 = 104$ are converted to themcorresponding ASCII codevalues$P_1 = M, P_2 = @, P_3 = t, P_4 = h$and hence get theoriginal plain text = "**M@th**"

V. TESTING AND ANALYSIS

The statistical analysis and frequency testing for this proposed method are presented.The graphs of the ElGamal algorithm and the proposed method ElGamal-MT are shown and compared here.In statistical analysis, we used ElGamal, MTand the proposed method ElGamal-MT of correlation coefficients.

A. Frequency Test

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

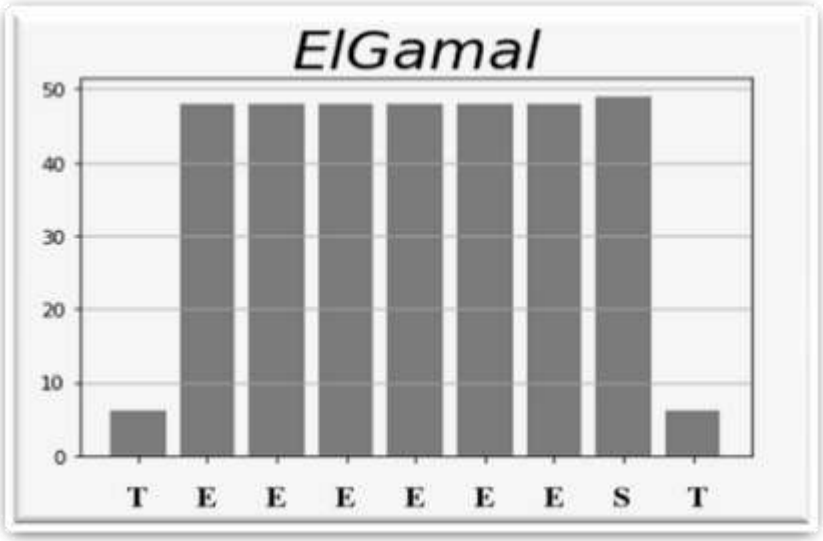

Fig. I: ElGamal algorithm ciphertext frequency distribution

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

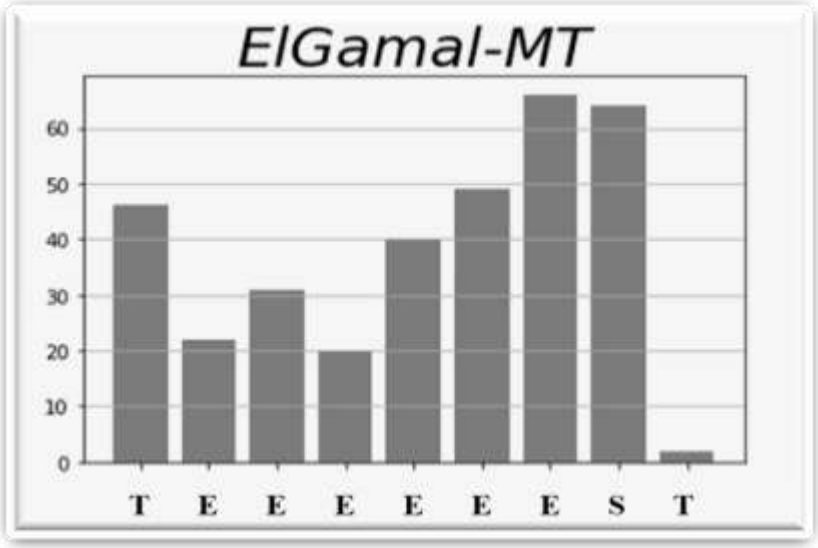

Fig. II: The proposed algorithm ciphertext frequency distribution

Figure III show that graphical representation of the frequency distribution shown in figures I and II for each algorithm.

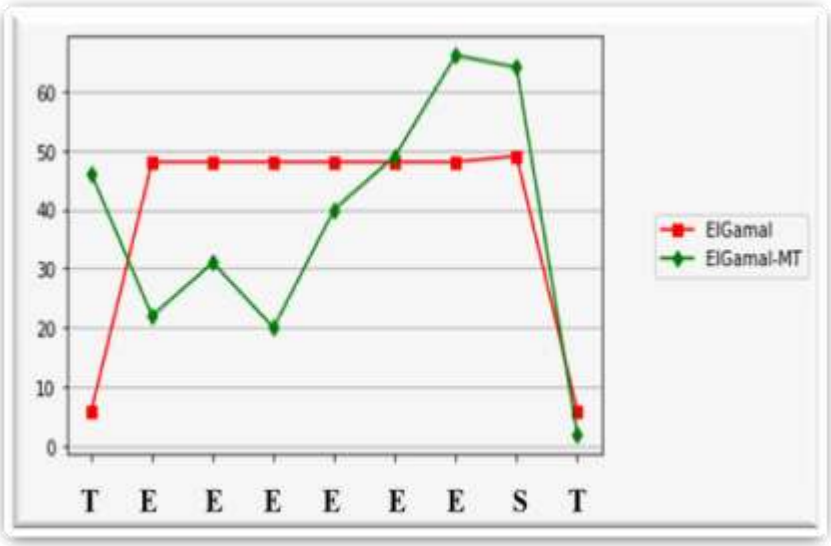

Fig. III: Ciphertext frequency distribution of ElGamal and ElGamal-MT

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

B. Statistical Analysis

Correlation coefficients are used in statistics to determine how closely two variables are related.The aim of the proposed method of research is to examine and create algorithm that strongly resists cryptographic attacks.The correlation demonstrates the relationship between two values.So, we examine the correlation coefficient between plaintext and ciphertext. If the correlation coefficient is one, plaintext and ciphertext are identical. If the correlation coefficient is zero, plaintext and ciphertext are completely different (i.e., good encryption). If the correlation coefficient is minus one, ciphertext is the inverse of plaintext. As a result, encryption success equates to smaller correlation coefficient values.The experimental results and correlation coefficient value of the proposed encryption algorithm are shown in the table.

Table: The Correlation test from plaintext to ciphertext

Message	Algorithm	Correlation
CryPto	ElGamal	0.52874287
	MT	-0.61845471
	ElGamal-MT	**0.20247775**
Ac@demic	ElGamal	-0.34380561
	MT	0.63134261
	ElGamal-MT	**0.25036787**
M@th	ElGamal	-0.72492244
	MT	-0.09195426
	ElGamal-MT	**-0.30975604**

The correlation test shows that the proposed method RSA-MT is more effective than RSA and MT. With the proposed method ElGamal-MT, correlation coefficient values are closer to zero.ElGamal or MT may perform better than ElGamal-MT for some data (message).Such circumstances and conditions that allow for generalization of performance are a research avenue to pursue.

VI. CONCLUSION

Cryptography is the process of encrypting data in order to ensure data transmission security.An applicationof Mellin Transform is a weak approach for cryptographic processes because encrypted data can be decrypted using basic 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 extends on an innovative method that employs the ElGamal algorithm in combination with the Mellin Transform. This method is difficult to break without knowing the private key. As a result, the proposed method combiningElGamal algorithm andMellin Transform can improve communication security.

REFERENCES

[1]. Allen B. (2008). “Implementing several attacks on plain ElGamal encryption”, Iowa State University.
[2]. Debnath L. and Bhatta D. (2015). “Integral Transforms and Their Applications” (Third Edition), 978-1-4822-2358-3.
[3]. 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.
[4]. ElGamal T. (1985). “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE transactions on information theory, 31(4), 469-472.
[5]. Grewal J. (2015). “ElGamal: Public-Key Cryptosystem”, Math and Computer Science Department, Indiana State University.
[6]. Johar M. Ashfaque (2019). “The Mellin Transform A Basic Introduction”, https://www.researchgate.net/publication/337465283
[7]. Malhotra M. and Singh A. (2013). “Study of various cryptographic algorithms”, International Journal of Scientific Engineering and Research, 1(3), 77-88.
[8]. Mohammadi M., Zolghadr A., Purmina M. A. (2018). “Comparison of two Public Key Cryptosystems”, Journal of Optoelectronical Nanostructures Summer, 3(3), 47-58.
[9]. 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).
[10]. Paar C. and Pelzl J. (2009). “Understanding cryptography: a textbook for students and practitioners”, Springer Science & Business Media.
[11]. Ranasinghe R. and Athukorala P. (2020). “A Generalization of the ElGamal public-key cryptosystem”, IACR Cryptol. ePrint Arch., 2020, 354.
[12]. Santana Y. C. (2014). “A Cryptographic Scheme of Mellin Transform”, arXiv preprint arXiv:1401.1232.
[13]. Singh M. M. P. and Saha M. (2017). “Application of Laplace - Mellin Transform to Cryptography”, International Journal of Mathematical Archive-8(7), 143-146.
[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.

Akash Thakkar. et. al. "Cryptographic method to enhance Data Security using ElGamal algorithm and Mellin Transform." *IOSR Journal of Mathematics (IOSR-JM)*, 18(6), (2022): pp. 12-18.