IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 24, Issue 3, Ser. III (May. –June. 2022), PP 08-14
www.iosrjournals.org

Cryptographic method to enhance the Data Security using ElGamal algorithm and Kamal 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 a popular technique to achieve confidentiality of information. Cryptography has two phases: Encryption and Decryption. Encryption is the process of transforming plaintext into ciphertext, whereas decryption is the reverse. Encryption and Decryption schemes based on applications of Kamal Transform are unable to provide more security to communicate the information. ElGamal algorithm is public key algorithm which depends on the discrete logarithm problem. This paper aims to introduce a method for cryptography using ElGamal algorithm and Kamal Transform to improve security of communication.*

Key word: *Cryptography, Plaintext, Ciphertext, Encryption, Decryption, ElGamal, Kamal Transform.*

Date of Submission: 05-06-2022 Date of Acceptance: 20-06-2022

I. Introduction

Cryptography is a technique of securing information. The procedures used to protect information in cryptography are developed from mathematical principles and a set of rule-based calculations referred to as algorithms. Encryption and Decryption are the two aspects of cryptography. Encryption is the process of scrambling data using a key generated by cryptographic algorithm whereas Decryption is the process of descrambling data using a key generated by cryptographic algorithm. Cryptography is mainly classified as three types:

- Symmetric key cryptography
- Asymmetric key cryptography
- Hash Function

In Symmetric key cryptography, the sender encrypts the data with a secret key and the receiver decrypts the data with the same key. Symmetric key cryptography is rapid and simple, but it has the drawback of requiring the sender and receiver to securely exchange keys. AES, Blowfish, DES, IDEA, RC4, Twofish are some Symmetric key algorithms.

Asymmetric key cryptography is also called as public key cryptography. In Asymmetric key cryptography a pair of keys is used to encrypt and decrypt the data. The data is encrypted using a public key and decrypted with a private key. ECC, ElGamal, DSA, Rabin, RSA are some Asymmetric key algorithms.

A. ElGamal Algorithm

ElGamal algorithm is public key algorithm developed by Taher ElGamal [3] 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 $(p,\ \alpha,\ \beta)$ 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 algorithm

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

In the process of Cryptography there is a contribution of some integral transforms. Encryption and Decryption schemes are developed by using properties of integral transforms.

B. Kamal Transform (KT)

Kamal Transform introduced by Kamal and Sedeeg [5] in 2016. Kamal Transform is derived from the classical Fourier integral and is widely used in applied mathematics and engineering fields.

Over the set of functions

$$A = \{ f(t)/\ \exists\ M, k_1, k_2 > 0\ , |\{f(t)\}| < M\ e^{|t|/k_j}, \text{if}\ t\ \epsilon\ (-1)^j\ \times [\ 0, \infty)\}$$

For a given function in the set A, the constant M must be finite number, k_1, k_2 may be finite or infinite.

Kamal Transform is defined by

$$K\ [\ f(t)] = G(v) = \int_0^\infty f(t) e^{-t/v}\ dt, t\ \geq 0, k_1\ \leq v\ \leq k_2 \qquad \ldots (1)$$

The variable v in this transform is used to factor the variable t in the argument of the function f.

Some standard functions:

For any function $f(t)$, we assume that the integral equation (1) exists.

1. Let $f(t) = 1$ then $K[1] = v$
2. Let $f(t) = t$ then $K[t] = v^2$
3. Let $f(t) = t^2$ then $K[t^2] = 2v^3 = 2!\, v^3$
4. In general case, if $n > 0$, then $K[t^n] = n!\, v^{n+1}$

Inverse Kamal Transform:

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

II. Literature Review

ElGamal [3] (1985) introduced a method of public key cryptosystem and signature scheme based on discrete logarithms. This new signature scheme together with an implementation of the Diffe-Hellman key distribution scheme that achieves a public key cryptosystem. 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.

Dissanayake [2] (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 (2015) [4] discussed ElGamal System which is a public key cryptosystem based on the discrete logarithm problem. He examined its security, advantages, disadvantages and its applications.

Kamal and Sedeeg [5] (2016) introduced a new integral transform namely Kamal Transform. They presented the definition and application of the Kamal transform and its solution of ordinary differential equations has been demonstrated.

Tayal et. al. [13] (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. 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.

Mittal and Gupta [7] (2019) developed a scheme in cryptography whose construction is based on the application of Kamal Transform. They presented the new cryptographic scheme using Kamal transform and congruence modulo operator involving ASCII value for encryption and decryption of message. The proposed algorithm is simple and straight forward.

Ranasinghe and Athukorala [12] (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. [10] (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 [14] (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.

III. Proposed Algorithm of the Mathematical Model

The proposed method is ElGamal algorithm with application of Kamal Transform (ElGamal-KT). 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 gives you an idea of how the proposed cryptographic scheme works.

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 $p(t)$ using primitive element α. i.e., $p(t) = \sum_{i=0}^{m} \alpha^i \ t^i$

B. Method of Encryption

Steps involved in Encryption as follows.

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 $\sum_{i=0}^{m} M_i(p(t))$

Step 3: Take Kamal Transform of a polynomial. i.e., $K\left[\sum_{i=0}^{m} M_i \ (p(t))\right] = \sum_{i=0}^{m} R_i \ v_i$

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

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 $C_0, C_1, \dots, C_m$

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 $R_i = m_i + (p * k_i)$ and get $R_0, R_1, \dots, R_m$

Step 6: Find the polynomial assuming R_i as a coefficient

Step 7: Apply inverse Kamal transform. i.e., $K^{-1}[\sum_{i=0}^{m} R_i\ v_i]$ and get $M_0, M_1, \dots, M_m$

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

In this section we are presented 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 $p(t)$ using primitive element $\alpha = 18$
i.e., $p(t) = \sum_{i=0}^{m} 18^i\ t^i$

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 = " **M@th** ", $P_0 = M, P_1 = @, P_2 = t, P_3 = h$,
convert into ASCII code integer $M_0 = 77, M_1 = 64, M_2 = 116, M_3 = 104$

Step 2: $\sum_{i=0}^{3} M_i(p(t)) = \sum_{i=0}^{3} M_i\, 18^i\, t^i = 77 + 1152 \cdot t + 37584 \cdot t^2 + 606528 \cdot t^3$

Step 3: $K\left[\sum_{i=0}^{3} M_i\ (p(t))\right] = K[77 + 1152 \cdot t + 37584 \cdot t^2 + 606528 \cdot t^3]$

$$= 77 \cdot v + 1! \cdot 1152 \cdot v^2 + 2! \cdot 37584 \cdot v^3 + 3! \cdot 606528 \cdot v^4$$

$$= 77 \cdot v + 1152 \cdot v^2 + 75168 \cdot v^3 + 3639168 \cdot v^4$$

$$= \sum_{i=0}^{3} R_i\ v_i$$

we get, $R_0 = 77, R_1 = 1152, R_2 = 75168, R_3 = 3639168$

Step 4: Find r_i such that $r_i \equiv R_i \ mod\ 67$,
we get, $r_0 = 10, r_1 = 13, r_2 = 61, r_3 = 63$

Step 5: Find k_i such that $k_i = (R_i - r_i)/67$,
we get, $k_0 = 1, k_1 = 17, k_2 = 1121, k_3 = 54315$

Step 6: Select $l = 21$

Step 7: Calculate ephemeral key $K_E \equiv \alpha^l \ mod\ p \equiv 18^{21} \ mod\ 67 = 43$

Step 8: Calculate masking key $K_M \equiv \beta^l \ mod\ p \equiv 14^{21} \ mod\ 67 = 24$

Step 9: Calculate cipher text $C_i \equiv R_i \cdot K_M \ mod\ 67$
we get, $C_0 = 39, C_1 = 44, C_2 = 57, C_3 = 38$

Step 10: Each integer of cipher text $C_0 = 39, C_1 = 44, C_2 = 57, C_3 = 38$ is converted to its construct by ASCII character $C_0 =$ '(Apostrophe) , $C_1 =$,(Comma), $C_2 = 9$, $C_3 =$ &(Ampersand) and stored as the cipher text C = " **',9&** "

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 = " **',9&** " converted to ASCII values of $C_0 = 39, C_1 = 44,$

$C_2 = 57, C_3 = 38$

Step 3: Calculate masking key $K_M \equiv {K_E}^d \ mod\ p \ \equiv 43^{12}\ mod\ 67 = 24$

Step 4: Each integer of $C_0 = 39, C_1 = 44, C_2 = 57, C_3 = 38$ is converted into
$m_i \equiv C_i \cdot (K_M)^{-1}\ mod\ p$
we get, $m_0 = 10, m_1 = 13, m_2 = 61, m_3 = 63$

Step 5: Calculate $R_i = m_i + (p * k_i)$
we have, $k_0 = 1, k_1 = 17, k_2 = 1121, k_3 = 54315$
we get, $R_0 = 77, R_1 = 1152, R_2 = 75168, R_3 = 3639168$

Step 6: The polynomial assuming $R_0 = 77, R_1 = 1152, R_2 = 75168, R_3 = 3639168$ as a coefficient $77 \cdot v + 1152 \cdot v^2 + 75168 \cdot v^3 + 3639168 \cdot v^4$

Step 7: Apply inverse Kamal transform,

$$K^{-1}[\sum_{i=0}^{3} R_i\ v_i] = K^{-1}[77 \cdot v + 1152 \cdot v^2 + 75168 \cdot v^3 + 3639168 \cdot v^4]$$
$$= 77 + (1152 \cdot t)/1! + (75168 \cdot t^2)/2! + (3639168 \cdot t^3)/3!$$
$$= 77 + 1152 \cdot t + 37584 \cdot t^2 + 606528 \cdot t^3$$

we get, $M_0 = 77, M_1 = 64, M_2 = 116, M_3 = 104$

Step 8: Each integer $M_0 = 77, M_1 = 64, M_2 = 116, M_3 = 104$ are converted to them corresponding ASCII code values $P_0 = M, P_1 = @, P_2 = t, P_3 = h$ and hence get the original plain text = " **M@th** "

V. Testing and Analysis

We present frequency testing and statistical analysis in this proposed method. The graph of ElGamal algorithm and proposed method ElGamal-KT is shown here and also compared with each other. We used ElGamal, KT and proposed method ElGamal-KT 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 plaintext and frequency level of ciphertext are considered on x-axis and y-axis respectively.

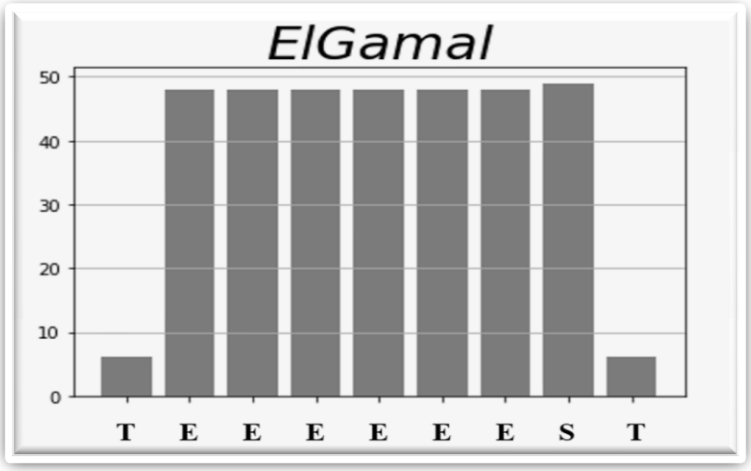

Fig. I: ElGamal algorithm ciphertext frequency distribution

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

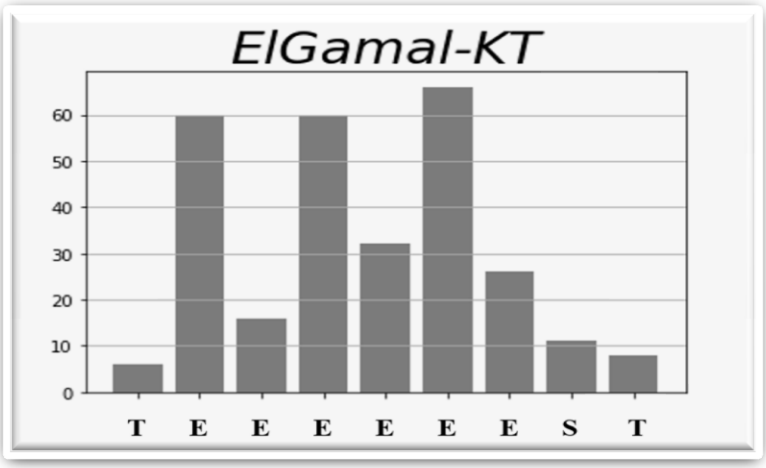

Fig. II: The proposed algorithm ciphertext frequency distribution

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

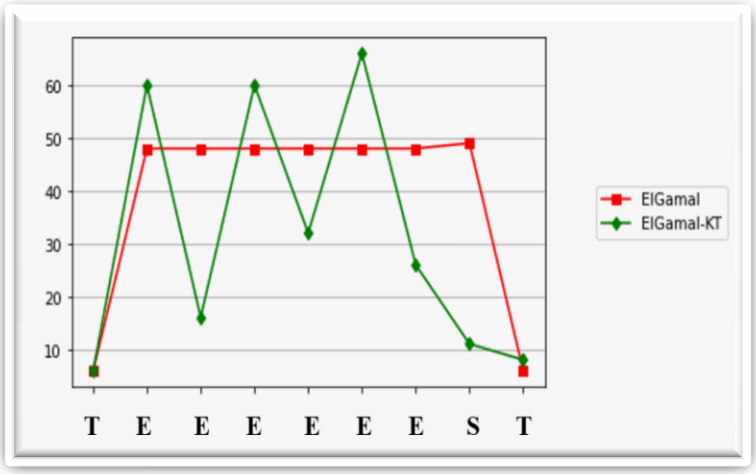

Fig. III: Ciphertext frequency distribution of ElGamal and ElGamal-KT

From the frequency test, each repeated character in a plaintext has different frequency after encryption using the proposed method ElGamal-KT.

B. Statistical Analysis

In statistics, correlation coefficients are used to measure how strong a relationship is between two of variables. The aim of the proposed method of research is to examine and create algorithm that strongly resists statistical attacks. The correlation shows associations between the pair of 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 table illustrates the experimental finding and the correlation coefficient value of the proposed encryption algorithm.

Table: The Correlation test from plaintext to ciphertext

Message	Algorithm	Correlation
M@th	ElGamal	-0.724922438
	KT	-0.85106901
	ElGamal-KT	**0.507970121**
CryPto	ElGamal	0.528742876
	KT	-0.481691431
	ElGamal-KT	**0.209138138**
Applied	ElGamal	0.015971677
	KT	-0.65370145
	ElGamal-KT	**-0.032797354**

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

VI. Conclusion

Cryptography is the process of encrypting data in order to ensure data transmission security. Use of the Kamal Transform for cryptographic process is a weak approach because encrypted data can be decrypted using basic modular arithmetic. ElGamal is a 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 Kamal Transform. Without knowing the private key, it is difficult to break this method. Therefore, this proposed method using ElGamal algorithm with Kamal Transform can provide more security of communication.

References

[1]. Allen B. (2008). "Implementing several attacks on plain ElGamal encryption", Iowa State University.
[2]. 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.
[3]. ElGamal T. (1985). "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE transactions on information theory, 31(4), 469-472.
[4]. Grewal J. (2015). "ElGamal: Public-Key Cryptosystem", Math and Computer Science Department, Indiana State University.
[5]. Kamal A. and Sedeeg H. (2016). "The new integral transform Kamal Transform", Advances in theoretical and applied mathematics, 11(4), 451-458.
[6]. Malhotra M. and Singh A. (2013). "Study of various cryptographic algorithms", International Journal of Scientific Engineering and Research, 1(3), 77-88.
[7]. Mittal A. and Gupta R. (2019). "Kamal Transformation based Cryptographic Technique in Network Security Involving ASCII Value", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, 8(12).
[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., Venkateswarlu K. (2019). "Enhancing the Data Security by Using RSA Algorithm with Application of Laplace Transform Cryptosystem", International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, 8(2).
[10]. 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).
[11]. Paar C. and Pelzl J. (2009). "Understanding cryptography: a textbook for students and practitioners", Springer Science & Business Media.
[12]. Ranasinghe R. and Athukorala P. (2020). "A Generalization of the ElGamal public-key cryptosystem", IACR Cryptol. ePrint Arch., 2020, 354.
[13]. 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.
[14]. 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.

Akash Thakkar, et. al. "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.