Original Article
ISSN (Online): 2456-8651

International Journal of Engineering Science Technologies
March-April 2023 7(2), 63–72

CRYPTOGRAPHIC METHOD TO ENHANCE DATA SECURITY USING RSA ALGORITHM AND MELLIN TRANSFORM

Akash Thakkar [1], Ravi Gor [2]

[1] Research scholar, Department of Applied Mathematical Science, Actuarial Science and Analytics, Gujarat University, India
[2] Department of Applied Mathematical Science, Actuarial Science and Analytics, Gujarat University, India

Received 11 March 2023
Accepted 10 April 2023
Published 26 April 2023

Corresponding Author

Akash Thakkar,
akashthakkar@gujaratuniversity.ac.in

DOI 10.29121/IJOEST.v7.i2.2023.490

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Cryptography is the technique of using mathematical algorithms to encrypt and decrypt the information. The process of converting plaintext to ciphertext is known as encryption, whereas the process of converting ciphertext to plaintext is known as decryption. Encryption and decryption methods based on Mellin Transform are unable to provide more security while transmitting the information. RSA algorithm is an Asymmetric key cryptography algorithm. The purpose of this study is to present a cryptographic method that uses the RSA algorithm and Mellin Transform to improve communication security.

Keywords: Cryptography, Encryption, Decryption, RSA Algorithm, Mellin Transform

1. INTRODUCTION THAKKAR AND GOR (2022), THAKKAR AND GOR (2022)

Cryptography is one of the most utilized techniques for data security. The techniques used to protect data in cryptography are based on mathematical concepts and a set of rule-based calculations known as algorithms. Two crucial cryptographic functions are encryption and decryption. Normal data is transformed into an unreadable form through encryption, and the reverse is accomplished through decryption. There are three main categories of cryptography:

- Symmetric key cryptography (secret key cryptography)

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

Symmetric key cryptography is a type of encryption where the same key is used to both encrypt and decrypt the data. Symmetric key cryptography is quick and easy, but it has the drawback that the sender and receiver must securely exchange keys. DES, AES, IDEA, RC4, Blowfish, Twofish are some Symmetric key algorithms.

Asymmetric key cryptography is also known as public-key cryptography. A pair of keys is used to encrypt and decrypt the data in Asymmetric key cryptography. Data is encrypted with the public key and decrypted with the corresponding private key. RSA, DSA, ElGamal, Rabin, ECC are some Asymmetric key algorithms.

1) RSA ALGORITHM Rivest (1978), Thakkar and Gor (2021)

RSA is public key cryptosystem developed by Rivest R., Shamir A., Adleman L. in 1978. RSA algorithm is widely used for secure data transmission. There are mainly three phases in RSA algorithm.

1) Key Generation
2) Encryption algorithm
3) Decryption algorithm

1) key Generation

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

1) Choose two prime numbers P and Q
2) Find N such that $N = P * Q$
3) Find the Phi of N, $\phi(N) = (P-1) * (Q-1)$
4) Choose an E such that $1 < E < \phi(N)$ and such that E and $\phi(N)$ share no divisors other than 1.
5) Determine D such that $E * D = 1 \left(mod\ \phi(N)\right)$

Public Key: $(E,\ N)$ and Private Key: (D)

2) Encryption algorithm

The process of converting Plain Text into Cipher Text is called as Encryption process.

$C = M^E\ mod\ (N)$

3) Decryption algorithm

The process of converting Cipher Text into Plain Text is called as Decryption process.

$M = C^D\ mod\ (N)$

Some integral transforms contribute to the process of cryptography. The features of integral transforms are used to create encryption and decryption methods.

2) MELLIN TRANSFORM (MT) Johar (2019), Santana (2014)

The Mellin Transform is an integral transform named after 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: $(\frac{d^k}{dx^k}\ f(x))^* = (-1)^k(s-k)_k f^*(s-k)$.
5) Where: $(s-k)_k = (s-k)(s-j+1)\ldots(s-1) = \frac{\Gamma(s)}{\Gamma(s-k)}$.
6) Convolution: $(\mathrm{f(x)g(x)})^* = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(z)G(s-z)dz$.

2. LITERATURE REVIEW

Rivest et al. (1978) introduced a method namely RSA to encrypt and decrypt the data. The RSA algorithm is the most widely used public key cryptography algorithm. One of the reason RSA has become most widely used is because it has two keys, one is for encryption and other one is for decryption. Thus, it is promising confidentiality, integrity, authenticity and non-repudiation of data.

Milanov (2009) concluded that RSA is a strong encryption algorithm that has stood a partial test of time. RSA is a public key cryptosystem that enables secure communications and digital signatures. Its security is based in part on the difficulty of factoring large numbers.

Malhotra & Singh (2013) studied various cryptographic algorithms. They provided a study of the research work done in cryptography field and various cryptographic algorithms being used. It is recapitulated that RSA is being used widely. This paper presented the current scenario and can provide a direction to naive users.

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

Lone and Uddin (2016) studied common attacks on RSA and its variants with possible countermeasures.

Nisha and Farik (2017) reviewed RSA public key cryptography algorithm. They examined its strengths and weaknesses and propose novel solutions to overcome the weakness.

Tayal et al. (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.

Mohammadi et al. (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.

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

Mok and Chuah (2019) studied brute force attack on RSA cryptosystem. They concluded that prime factorization attack is the most efficient way on RSA cryptanalysis.

Nagalakshmi et al. (2019) provided the conditions for the RSA Cryptosystem based on the Laplace transform techniques. The proposed algorithm was implemented using a high-level programme, and its time complexity was tested using RSA cryptosystem algorithms. The comparison shows that the proposed algorithm improves data security when compared to RSA cryptosystem algorithms and the use of the Laplace transform in cryptosystem schemes.

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

Thakkar and Gor (2022) presented 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 (2022) provided 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 paper.

3. PROPOSED ALGORITHM OF THE MATHEMATICAL MODEL

The proposed method is RSA algorithm with application of Mellin Transform (RSA-MT). 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 four large random prime numbers p, q, r, s

Step 2: Calculate $n = p * q * r * s$ and $\phi(n) = (p-1) * (q-1) * (r-1) * (s-1)$

Step 3: Select the public exponent f, $1 < f < \phi(n)$ such that gcd $(f, \phi(n)) = 1$

Step 4: Find the secret exponent d, $1 < d < \phi(n)$ such that $d * f \equiv 1 \ (mod\ \phi(n))$

Step 5: Generate polynomial $p(x)$ using public exponent f. i.e., $p(x) = \sum_{i=1}^{m} f^i x^i$

2) Method of Encryption

Following are the steps involved in Encryption.

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 $r_i \equiv R_i \ mod\ n$

Step 7: Find k_i such that $k_i = (R_i - r_i)/n$ and $k_0 =$ (value of s)

Step 8: Calculate cipher text $C_i = {R_i}^f \ mod\ n$ then get integer of cipher text $C_1, C_2, \dots, C_m$

Step 9: Each integer of cipher text $C_1, C_2, \dots, C_m$ 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 $C_1, C_2, \dots, C_m$

Step 3: Each integer of $C_1, C_2, \dots, C_m$ is converted into $m_i = {C_i}^d \ mod\ n$ and get $m_1, m_2, \dots, m_m$

Step 4: Calculate $R_i = m_i + (n * k_i)$ and get $R_1, R_2, \dots, R_m$

Step 5: Find the polynomial assuming R_i as a coefficient

Step 6: 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 7: Each integer M_i are converted to their corresponding ASCII code values and hence get the original plain text $P_1, P_2, \dots, P_m$

Public key: $\{p(x), n, f, k_i\}$

Private key: $\{d\}$

4. 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.

Step 1: Primes $p = 11, q = 13, r = 17, s = 19$

Step 2: $n = 46189$ and $\phi(n) = 34560$

Step 3: $f = 23, 1 < 23 < 34560$ such that gcd $(23, 34560) = 1$

Step 4: $d = 27047, \quad 1 < 27047 < 34560$ such that $27047 * 23 \equiv 1\ (mod\ 34560)$

Step 5: Polynomial $p(x)$ using public exponent $f = 23$

i.e., $p(x) = \sum_{i=1}^{m} 23^i\ x^i$

Bob then sends his public key $(p(x), n, f)$ 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: $\sum_{i=1}^{4} M_i\big(p(x)\big) = \sum_{i=1}^{4} M_i(\ 23^i\ x^i)$

$= 1771 \cdot x + 33856 \cdot x^2 + 1411372 \cdot x^3 + 29103464 \cdot x^4$

Step 3: $L(x) = \sum_{i=1}^{4} e^{-x}\ \left[M_i\left(23^i\ x^i\right)\right]$

$= e^{-x}\ [1771 \cdot x + 33856 \cdot x^2 + 1411372 \cdot x^3 + 29103464 \cdot x^4]$

we get, $G_1 = 1771, G_2 = 33856, G_3 = 1411372, G_4 = 29103464$

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, $R_1 = 10626, R_2 = 812544, R_3 = 169364640, R_4 = 20954494080$

Step 6: Find r_i such that $r_i \equiv R_i\ mod\ 46189$,

we get, $r_1 = 10626, r_2 = 27331, r_3 = 35766, r_4 = 22828$

Step 7: Find k_i such that $k_i = (R_i - r_i)/46189$ and $k_0 =$ 3 (value of s)

we get, $k_1 = 0, k_2 = 17, k_3 = 3666, k_4 = 453668$

Step 8: Calculate cipher text $C_i = {R_i}^f\ mod\ 46189$,

we get, $C_1 = 15114, C_2 = 5260, C_3 = 620, C_4 = 10257$

Step 9: Each integer of cipher text $C_1 = 15114, C_2 = 5260, C_3 = 620, C_4 = 10257$ is converted to its construct by ASCII character $C_1 =$ 曼, $C_2 =$ Ċ, $C_3 =$ ł, $C_4 =$ ∵ and stored as the cipher text $C =$ " **曼Ċł∵** "

Alice then sends (k_i, 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 $C =$ " **曼Ċł∵** " converted to ASCII values of

$C_1 = 15114, C_2 = 5260, C_3 = 620, C_4 = 10257$

Step 3: Each integer of $C_1 = 15114, C_2 = 5260, C_3 = 620, C_4 = 10257$ is converted into

$m_i = {C_i}^d\ mod\ 46189$,

we get, $m_1 = 10626, m_2 = 27331, m_3 = 35766, m_4 = 22828$

Step 4: Calculate $R_i = m_i + (n * k_i)$,

we have, $k_1 = 0, k_2 = 17, k_3 = 3666, k_4 = 453668$

we get, $R_1 = 10626, R_2 = 812544, R_3 = 169364640, R_4 = 20954494080$

Step 5: The polynomial assuming $R_1 = 10626, R_2 = 812544, R_3 = 169364640, R_4 = 20954494080$ as a coefficient

$10626 * x + 812544 * x^2 + 169364640 * x^3 + 20954494080 * x^4$

Step 6: Apply inverse Mellin Transform

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

$= e^{-x} [10626 * x + 812544 * x^2 + 169364640 * x^3 + 20954494080 * x^4]$

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 7: Each integer $M_1 = 77, M_2 = 64, M_3 = 116, M_4 = 104$ are converted to them

corresponding ASCII code values $P_1 = M, P_2 = @, P_3 = t, P_4 = h$ and hence get the

original plain text = " **M@th** "

5. TESTING AND ANALYSIS THAKKAR AND GOR (2022), THAKKAR AND GOR (2022)

The statistical analysis and frequency testing for this proposed method are presented. The graph of RSA algorithm and proposed method RSA-MT is shown here and also compared with each other. In statistical analysis, correlation coefficients are obtained for RSA, MT, and the proposed RSA-MT.

1) Frequency Test

Figure 1 show that the frequency of the same character in plaintext after encryption with RSA algorithm is the same, where the x-axis and y-axis represent plaintext and frequency level of ciphertext, respectively.

Figure 1

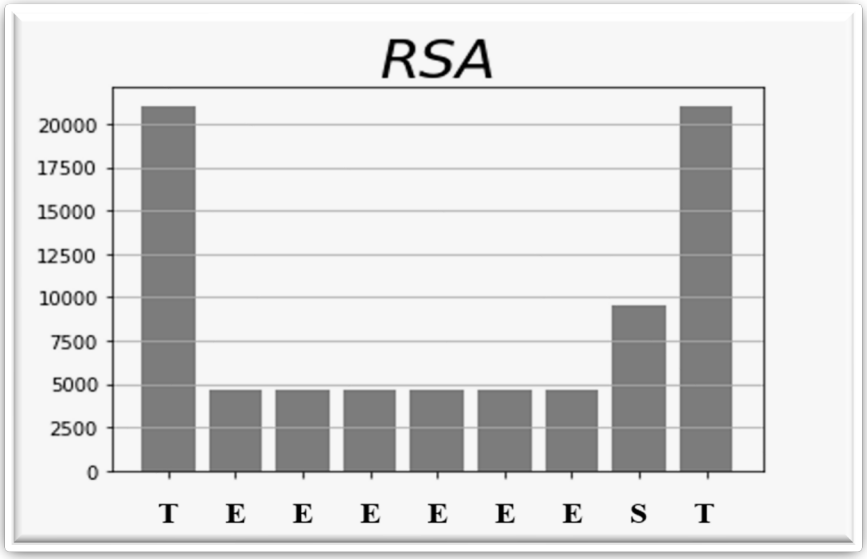

Figure 1 RSA Algorithm Ciphertext Frequency Distribution

Figure 2 demonstrate that the frequency of each character in a plaintext change after encryption with the proposed method RSA-MT, where the x-axis and y-axis represent plaintext and frequency level of ciphertext, respectively.

Figure 2

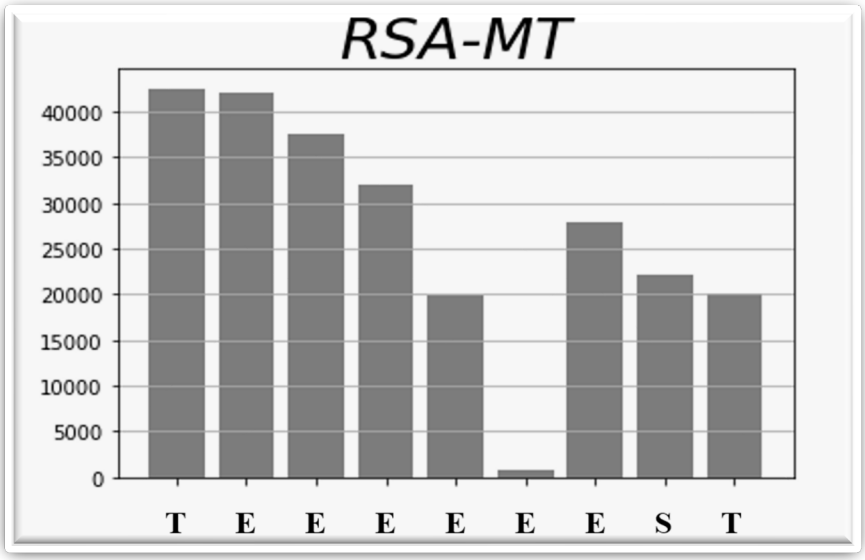

Figure 2 The Proposed Algorithm Ciphertext Frequency Distribution

Figure 3 show that graphical representation of the frequency distribution shown in Figure 1 and Figure 2 for each algorithm.

Figure 3

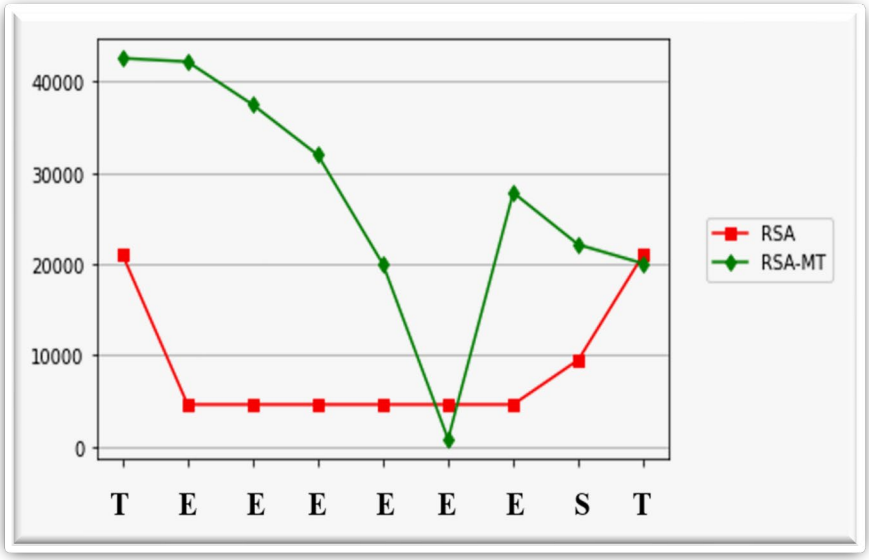

Figure 3 Ciphertext Frequency Distribution of RSA And RSA-MT

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

2) 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 shows the relationship between two values. The correlation coefficient between 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 and the correlation coefficient value of the proposed encryption method.

Table 1

Table 1 The Correlation Test from Plaintext to Ciphertext

Message	Algorithm	Correlation
Applied	RSA	0.19820314
	MT	0.67223518
	RSA-MT	**0.05420039**
CryPto	RSA	0.67704516
	MT	-0.61845471
	RSA-MT	**0.29986904**
M@th	RSA	0.91830612
	MT	-0.09195426
	RSA-MT	**-0.40369100**

According to the correlation test, proposed method RSA-MT is more effective than RSA and MT. Correlation coefficient values are closer to zero with the proposed method RSA-MT. However, for specific types of data (messages), RSA or MT may outperform RSA-MT. Such circumstances and conditions under which performance can be generalized are a research path to pursue.

6. CONCLUSION

One of the most crucial foundational technologies for ensuring the security of data communication is cryptography. An application of Mellin Transform for cryptography is a weak strategy since encrypted data can be deciphered using simple modular arithmetic. RSA is most widely used technique for keeping data secret. The primary method of breaking RSA still depends on how quickly huge prime numbers can be factored. The proposed research based on innovative approach that combines RSA algorithm with Mellin Transform of function to generate four huge prime numbers. Without having access to the private key, it is challenging to crack this method. As a result, the proposed method combining RSA algorithm and Mellin Transform has the potential to improve communication security.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Debnath, L., and Bhatta, D. (2015). "Integral Transforms and their Applications" (3rd ed.).

Johar, M. Ashfaque (2019). "The Mellin Transform à Basic Introduction".

Lone, A. H. and Uddin, M. (2016). "Common Attacks on RSA and its Variants with Possible Countermeasures". International Journal of Research in Management and Technology, 5, 65-70.

Malhotra, M. & Singh, A. (2013). "Study of Various Cryptographic Algorithms". International Journal of Scientific Engineering and Research, 1(3), 77-88.

Milanov, E. (2009). "The RSA Algorithm". RSA Laboratories, 1-11.

Mohammadi, M., Zolghadr, A., and Purmina, M. A. (2018). "Comparison of two Public Key Cryptosystems". Journal of Optoelectronical Nanostructures Summer, 3(3), 47-58. https://dorl.net/dor/20.1001.1.24237361.2018.3.3.5.0

Mok, C. J. and Chuah, C. W. (2019). "An Intelligence Brute Force Attack on RSA Cryptosystem". Communications in Computational and Applied Mathematics, 1(1).

Nagalakshmi, G., Sekhar, A. C., Sankar, N. R., and 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), 8(2).

Nisha, S., and Farik, M. (2017). "RSA Public Key Cryptography Algorithm–A Review". International Journal of Scientific & Technology Research, 6(7), 187-191.

Rivest, R., Shamir, A., and Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM, 21(2), 120-126. https://doi.org/10.1145/359340.359342.

Santana, Y. C. (2014). "A Cryptographic Scheme of Mellin Transform".

Singh, M. M. P. and Saha, M. (2017). "Application of Laplace - Mellin Transform to Cryptography". International Journal of Mathematical Archive-8(7), 143-146.

Stallings, W. (2002). "Cryptography and Network Security" (3rd ed). Pearson Education.

Tayal, S., Gupta, N., Gupta, P., Goyal, D., and Goyal, M. (2017). "A Review Paper on Network Security and Cryptography". Advances in Computational Sciences and Technology, 10(5), 763-770.

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, 324-331.

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), 12-18.

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), 01-07.

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), 08-14.