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 01-07
www.iosrjournals.org

Cryptographic method to enhance the Data Security using RSA 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
[1]akashthakkar@gujaratuniversity.ac.in

Abstract: *Cryptography includes two phases: Encryption and Decryption. Encryption and Decryption schemes based on Kamal Transform are unable to provide more security to communicate the information. RSA (Rivest–Shamir–Adleman) algorithm is a popular public key algorithm. RSA cryptosystem is based on the difficulty of factoring large integers. This paper aims to introduce a method for cryptography using RSA algorithm and Kamal Transform to improve security of communication.*

Key Word: *Cryptography, Encryption, Decryption, RSA, Kamal Transform.*

Date of Submission: 03-06-2022 Date of Acceptance: 17-06-2022

I. Introduction

One of the extensively used methods for information security is cryptography. Cryptography is a Greek word that means the art of turning information into an unreadable format. Encryption and Decryption are two essential functionalities of cryptography. Encryption is the process of changing readable data into an unreadable form, whereas decryption is the process of returning the unreadable data to its original state. Cryptography can be broken down into three different types:

- Symmetric key cryptography (Secret key cryptography)
- Asymmetric key cryptography (Public key cryptography)
- Hash Function

Symmetric key cryptography is an encryption method in which the data is encrypted and decrypted using the same key. Symmetric key cryptography is quick and easy, but it has the disadvantage of requiring the sender and receiver to securely exchange keys. DES, AES, IDEA, RC4, Blowfish, Twofish are some Symmetric key algorithms.

Asymmetric key cryptography, often known as public key cryptography, is a method of encrypting and decrypting data and protecting it from unauthorized access by using a pair of related keys - one public key and one private key. RSA, DSA, ElGamal, Rabin, ECC are some Asymmetric key algorithms.

A. RSA Algorithm

RSA is public key cryptosystems developed by Rivest R., Shamir A., Adleman L. [11] in 1978. RSA algorithm is widely used for secure data transmission. There are mainly three steps 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.

a) Choose two prime numbers P and Q
b) Find N such that $N = P * Q$
c) Find the Phi of N, $\phi(N) = (P-1)*(Q-1)$
d) Choose an E such that $1 < E < \phi(N)$ and such that E and $\phi(N)$ share no divisors other than 1
e) Determine D such that $E * D = 1 \left(mod\, \phi(N)\right)$

Now, the public key consists of public key exponent E and N and private key consists of private key exponent D and N.

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

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

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 was introduced by Kamal and Sedeeg [1] in 2016. Kamal Transform is derived from the Fourier integral and is widely utilized in applied mathematics and engineering.

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

Rivest et. al. [11] (1978) introduced a method namely RSA for how 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 [4] (2009) concluded that RSA is a strong encryption algorithm that has stood a partial test of time. RSA implements a public key cryptosystem that allows secure communications and digital signatures and its security rests in part on the difficulty of factoring large numbers.

Malhotra and Singh [3] (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.

Kamal and Sedeeg [1] (2016) introduced a new integral transform namely Kamal Transform. They presented the definition and application of Kamal Transform and its solution of ordinary differential equations has been demonstrated.

Lone and Uddin [2] (2016) studied common attacks on RSA and its variants with possible countermeasures.

Nisha and Farik [10] (2017) reviewed RSA public key cryptography algorithm. They examined its strengths and weaknesses and propose novel solutions to overcome the weakness.

Tayal [12] et. al. (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 reasons.

Mohammadi [6] et. al. (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 [5] (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.

Mok and Chuah [7] (2019) studied brute force attack on RSA cryptosystem. They concluded that prime factorization attack is the most efficient way on RSA cryptanalysis.

Nagalakshmi [8] et. al. (2019) provided the conditions that give rise to the RSA Cryptosystem based on the Laplace transform techniques. The proposed algorithm is implemented using a high-level program and time complexity of the proposed algorithm is tested with RSA cryptosystem algorithms. The comparison reveals that the proposed algorithm enhances the data security as compare with RSA cryptosystem algorithms and application of Laplace transform for cryptosystem scheme.

Thakkar and Gor [13] (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 RSA algorithm with application of Kamal Transform (RSA-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 an insight into the proposed cryptographic scheme.

A. Method of Key Generation

Steps involved in Key Generation as follows.

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 e, $1 < e < \phi(n)$ such that gcd $(e, \phi(n)) = 1$

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

Step 5: Generate polynomial $p(t)$ using public exponent e. i.e., $p(t) = \sum_{i=0}^{m} e^i\, t^i$

B. Method of Encryption

Steps involved in Encryption as follows.

Step 1: Select the plain text $P_0, P_1, \dots, P_m$ and 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 $r_i \equiv\ R_i\ mod\ n$

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

Step 6: Calculate cipher text $C_i =\ R_i{}^e\ mod\ n$ then get integer of cipher text $C_0, C_1, \dots, C_m$

Step 7: Each integer of cipher text $C_0, C_1, \dots, C_m$ is converted to its construct by ASCII character is 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: Each integer of $C_0, C_1, \dots, C_m$ is converted into $m_i =\ C_i{}^d\ mod\ n$ and get $m_0, m_1, \dots, m_m$

Step 4: Calculate $R_i = m_i + (n * k_i)$ and get $R_0, R_1, \dots, R_m$

Step 5: Find the polynomial assuming R_i as a coefficient

Step 6: Apply inverse Kamal Transform. i.e., $K^{-1}[\sum_{i=0}^{m} R_i\, v_i]$ and get integer $M_0, M_1, \dots, M_m$
Step 7: Each integer M_i are converted to their corresponding ASCII code values and hence get the original plain text $P_0, P_1, \dots, P_m$

Public key: $\{p(t), n, e, k_i\}$
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: Primes $p = 11, q = 13, r = 17, s = 19$
Step 2: $n = 46189$ and $\phi(n) = 34560$
Step 3: $e = 23$, $1 < 23 < 34560$ such that gcd $(23, 34560) = 1$
Step 4: $d = 27047$, $1 < 27047 < 34560$ such that $27047 * 23 \ \equiv 1\ (mod\ 34560)$
Step 5: Polynomial $p(t)$ using public exponent $e = 23$
i.e., $p(t) = \sum_{i=0}^{m} 23^i\, t^i$

Bob then sends his public key $(p(t), n, e)$ 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: $\sum_{i=0}^{3} M_i\big(p(t)\big) = \sum_{i=0}^{3} M_i\, 23^i\, t^i = 77 + 1472 \cdot t + 61364 \cdot t^2 + 1265368 \cdot t^3$
Step 3: $K\left[\sum_{i=0}^{3} M_i\,\big(p(t)\big)\right] = K[77 + 1472 \cdot t + 61364 \cdot t^2 + 1265368 \cdot t^3]$
$= 77 \cdot v + 1! \cdot 1472 \cdot v^2 + 2! \cdot 61364 \cdot v^3 + 3! \cdot 1265368 \cdot v^4$
$= 77 \cdot v + 1472 \cdot v^2 + 122728 \cdot v^3 + 7592208 \cdot v^4$
$= \sum_{i=0}^{3} R_i\, v_i$
we get, $R_0 = 77, R_1 = 1472, R_2 = 122728, R_3 = 7592208$
Step 4: Find r_i such that $r_i \equiv\ R_i\ mod\ 46189$,
we get, $r_0 = 77, r_1 = 1472, r_2 = 30350, r_3 = 17212$
Step 5: Find k_i such that $k_i = (R_i - r_i)/46189$,
we get, $k_0 = 0, k_1 = 0, k_2 = 2, k_3 = 164$
Step 6: Calculate cipher text $C_i =\ {R_i}^e\ mod\ 46189$,
we get, $C_0 = 21813, C_1 = 10409, C_2 = 17282, C_3 = 9620$
Step 7: Each integer of cipher text $C_0 = 21813, C_1 = 10409, C_2 = 17282, C_3 = 9620$ is converted to its construct by ASCII character $C_0 =$唵, $C_1 =$⢩, $C_2 =$狍, $C_3 =$▔ and stored as the cipher text $C =$ " **唵**⢩狍▔ "

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 $C =$ " **唵**⢩狍▔ " converted to ASCII values of
$C_0 = 21813, C_1 = 10409, C_2 = 17282, C_3 = 9620$
Step 3: Each integer of $C_0 = 21813, C_1 = 10409, C_2 = 17282, C_3 = 9620$ is converted into $m_i =\ {C_i}^d\ mod\ 46189$, we get, $m_0 = 77, m_1 = 1472, m_2 = 30350, m_3 = 17212$
Step 4: Calculate $R_i = m_i + (n * k_i)$,
we have, $k_0 = 0, k_1 = 0, k_2 = 2, k_3 = 164$
we get, $R_0 = 77, R_1 = 1472, R_2 = 122728, R_3 = 7592208$
Step 5: The polynomial assuming $R_0 = 77, R_1 = 1472, R_2 = 122728, R_3 = 7592208$ as a coefficient $77 \cdot v + 1472 \cdot v^2 + 122728 \cdot v^3 + 7592208 \cdot v^4$
Step 6: Apply inverse Kamal Transform,
$K^{-1}[\sum_{i=0}^{3} R_i\, v_i] = K^{-1}[77 \cdot v + 1472 \cdot v^2 + 122728 \cdot v^3 + 7592208 \cdot v^4]$
$= 77 + (1472 \cdot t)/1! + (122728 \cdot t^2)/2! + (7592208 \cdot t^3)/3!$
$= 77 + 1472 \cdot t + 61364 \cdot t^2 + 1265368 \cdot t^3$
and get integer $M_0 = 77, M_1 = 64, M_2 = 116, M_3 = 104$

Step 7: 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 RSA algorithm and proposed method RSA-KT is shown here and also compared with each other. We used RSA, KT and proposed method RSA-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 RSA algorithm is the same, where plaintext and frequency level of ciphertext are considered on x-axis and y-axis respectively.

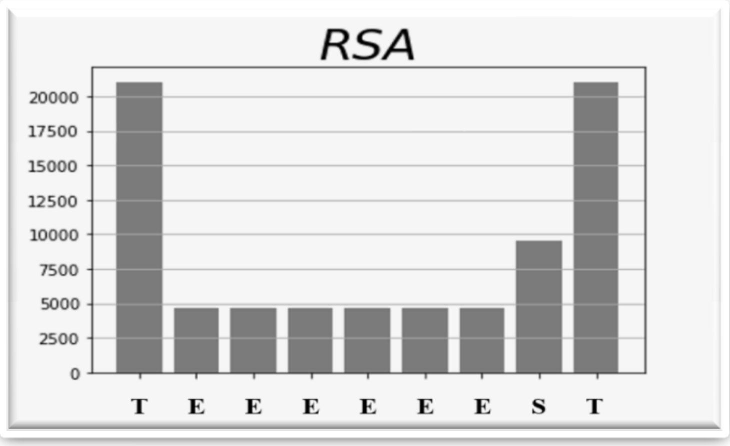

Fig. I: RSA algorithm ciphertext frequency distribution

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

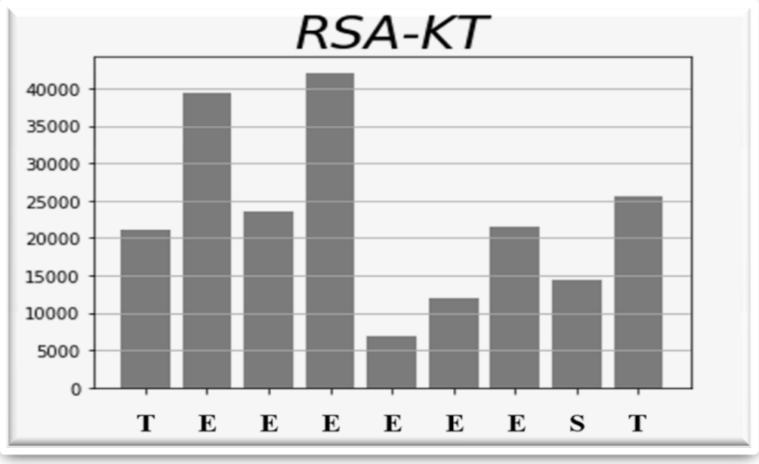

Fig. II: The proposed algorithm ciphertext frequency distribution

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

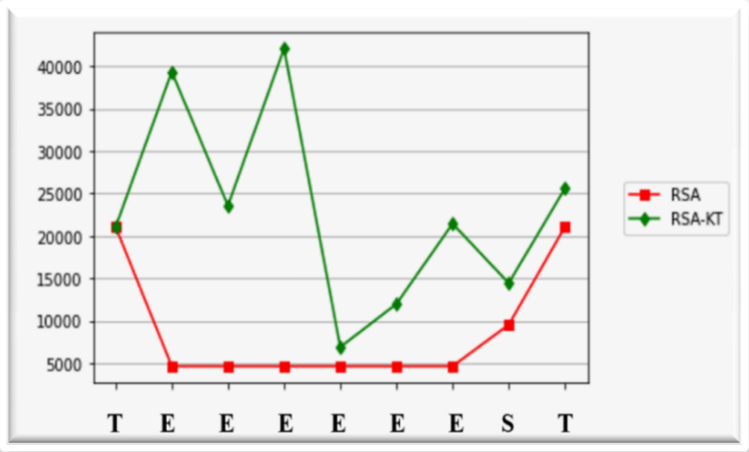

Fig. III: Ciphertext frequency distribution of RSA and RSA-KT

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

B. *Statistical Analysis*

In statistics, correlation coefficients are used to determine how strong a relationship exists between two 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	RSA	0.91830612
	KT	-0.85106901
	RSA-KT	**0.03600911**
Applied	RSA	0.198203144
	KT	-0.65370145
	RSA-KT	**-0.134557711**
CryPto	RSA	0.67704516
	KT	-0.481691431
	RSA-KT	**-0.400916969**

From the correlation test, proposed method RSA-KT gives better result from RSA and KT. Correlation coefficient values are closer to zero with RSA-KT algorithm. However, for some data (message), RSA or KT may perform better than RSA-KT. 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 Kamal Transform for cryptographic process is a weak scheme because encrypted data can be decrypted by elementary modular arithmetic. RSA is most widely used technique for keeping data secret. Breaking of RSA algorithm is dependent on speed of factorization of large prime numbers. The proposed work is based on a unique strategy that combines the RSA algorithm with Kamal Transform of function providing four large prime integers. It is impossible to break this method without knowing the private key. Therefore, this proposed method using RSA algorithm with Kamal Transform can provide more security of communication.

References

[1]. Kamal A. and Sedeeg H. (2016). “The new integral transform: Kamal Transform”, Advances in theoretical and applied mathematics, 11(4), 451-458.

[2]. 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.

[3]. Malhotra M. and Singh A. (2013). "Study of various cryptographic algorithms", International Journal of Scientific Engineering and Research, 1(3), 77-88.

[4]. Milanov E. (2009). "The RSA algorithm". RSA Laboratories, 1-11.

[5]. 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).

[6]. Mohammadi M., Zolghadr A., Purmina M. A. (2018). "Comparison of two Public Key Cryptosystems", Journal of Optoelectronical Nanostructures Summer, 3(3), 47-58.

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

[8]. 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).

[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]. Nisha S. and Farik M. (2017). "RSA Public Key Cryptography Algorithm–A Review", International journal of scientific & technology research, 6(7), 187-191.

[11]. Rivest R., Shamir A., Adleman L. (1978). "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, 21(2), 120-126.

[12]. 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.

[13]. 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.

[14]. William Stallings. "Cryptography and Network Security", ISBN 81-7758-011-6, Pearson Education, Third Edition.

Akash Thakkar, et. al. "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.