Quest Journals
Journal of Research in Applied Mathematics
Volume 9 ~ Issue 4 (2023) pp: 48-54
ISSN(Online) : 2394-0743 ISSN (Print): 2394-0735
www.questjournals.org

Research Paper

Cryptographic method to enhance the Data Security using RSA 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 is divided into two stages: encryption and decryption. Encryption is the process of transforming plaintext to ciphertext, whereas decryption is the reverse procedure. RSA (Rivest–Shamir–Adleman) algorithm is popular public-key algorithm. Sumudu Transform-based encryption and decryption systems are not capable of providing more security in sharing information. The objective of this study is to introduce a cryptographic method using both RSA algorithm and Sumudu Transform to improve security of communication.*
KEYWORDS: *Cryptography, Encryption, Decryption, RSA, Sumudu Transform.*

R*eceived 12 Apr., 2023;* ***R****evised 25 Apr., 2023;* ***A****ccepted 27 Apr., 2023 © The author(s) 2023.*
P*ublished with open access at* ***www.questjournals.org***

I. INTRODUCTION

A popular method for information security is cryptography. Cryptography involves the use of algorithms and mathematical techniques to transform plaintext (the original message) into ciphertext (the encrypted message). The process of converting plaintext into ciphertext is known as encryption and the process of converting ciphertext into plaintext is known as decryption. There are several types of cryptography techniques including symmetric key cryptography, asymmetric key cryptography and hashing.

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. RSA Algorithm

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 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 $E * D = 1 \left(mod\ \phi(N)\right)$

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

(2) Encryption algorithm
The process of converting plaintext into ciphertext is called as encryption process.
$C = M^E \ mod\ N$

(3) Decryption algorithm
The process of converting ciphertext into plaintext 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. Sumudu Transform (ST)

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

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

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$S[t^n] = n!\, u^n$.

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

Rivest et. al. [10] (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.

Watugala [17] (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 [3] (2002) discussed the general properties of the Sumudu Transform and some special functions that occur frequently in physical and engineering applications.

Milanov [5] (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 [4] (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.

Bodkhe and Panchal [1] (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.

Nisha and Farik [9] (2017) reviewed RSA public key cryptography algorithm. They examined its strengths and weaknesses and propose novel solutions to overcome the weakness.

Tayal et. al. [12] (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 [2] (2017) analyzed security based on Sumudu Transform in cryptography and concluded that without knowing the key, the encrypted text can be decrypted.

Mohammadi et. al. [6] (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.

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 et. al. [8] (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 [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.

Thakkar and Gor [14] (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 [15] (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 [16] (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 [17] (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.

III. PROPOSED ALGORITHM OF THE MATHEMATICAL MODEL

The proposed method is RSA algorithm with application of Sumudu Transform (RSA-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.

A. 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 $p(t)$ using public exponent f.i.e., $p(t) = \sum_{i=0}^{m} f^{i+3} t^{i+3}$

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

Private key: $\{d\}$

B. Method of Encryption

Following are the steps involved in Encryption.

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 Sumudu Transform of a polynomial. i.e., $S\left[\sum_{i=0}^{m} M_i\ (p(t))\right] = \sum_{i=0}^{m} R_i u^{i+3}$

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 $C_i = {R_i}^f \ mod\ n$ 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

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: 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 Sumudu Transform. i.e., $S^{-1}[\sum_{i=0}^{m} R_i u^{i+3}]$ 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 $P_0, P_1, \dots, P_m$

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.
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: $d = 27047,\ 1 < 27047 < 34560$ such that $27047 * 23 \equiv 1\ (mod\ 34560)$
Step 5: Polynomial $p(t)$ using public exponent $f = 23$
i.e., $p(t) = \sum_{i=0}^{m} 23^{i+3} t^{i+3}$

Bob then sends his public key $(p(t), n, f)$ to Alice.
Alice computes his parameters to encrypt the message using steps as given in method of Encryption.
Step 1: Plain text = " **M@th** ", $P_0 = M, P_1 = @, P_2 = t, P_3 = h,$
convert into ASCII code integer $M_0 = 77, M_1 = 64, M_2 = 116, M_3 = 104$
Step 2: $\sum_{i=0}^{3} M_i\big(p(t)\big) = \sum_{i=0}^{3} M_i 23^{i+3} t^{i+3}$

$$= 936859 \cdot t^3 + 17909824 \cdot t^4 + 746615788 \cdot t^5 + 15395732456 \cdot t^6$$

Step 3: $S\left[\sum_{i=0}^{3} M_i\big(p(t)\big)\right] = S\left[936859 \cdot t^3 + 17909824 \cdot t^4 + 746615788 \cdot t^5 + 15395732456 \cdot t^6\right]$

$$= 3! \cdot 936859 \cdot u^3 + 4! \cdot 17909824 \cdot u^4 + 5! \cdot 746615788 \cdot u^5 + 6! \cdot 15395732456 \cdot u^6$$

$$= 5621154 \cdot u^3 + 429835776 \cdot u^4 + 89593894560 \cdot u^5 + 11084927368320 \cdot u^6$$

$$= \sum_{i=0}^{3} R_i u^{i+3}$$

we get, $R_0 = 5621154, R_1 = 429835776, R_2 = 89593894560, R_3 = 11084927368320$
Step 4: Find r_i such that $r_i \equiv R_i\ mod\ 46189$,
we get, $r_0 = 32285, r_1 = 942, r_2 = 28913, r_3 = 20683$
Step 5: Find k_i such that $k_i = (R_i - r_i)/46189$,
we get,$k_0 = 121, k_1 = 9306, k_2 = 1939723, k_3 = 239990633$
Step 6: Calculate cipher text $C_i = {R_i}^f\ mod\ 46189$,
we get,$C_0 = 18029, C_1 = 6030, C_2 = 17395, C_3 = 34853$
Step 7: Each integer of cipher text $C_0 = 18029, C_1 = 6030, C_2 = 17395, C_3 = 34853$are converted to its construct by ASCII character $C_0 =$ 襆, $C_1 =$ ﻕ, $C_2 =$ 脈, $C_3 =$ 蠻 and stored as the cipher text $C =$ "**襆ﻕ脈蠻**"

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 $C =$ "**襆ﻕ脈蠻**" converted to ASCII values of

$$C_0 = 18029, C_1 = 6030, C_2 = 17395, C_3 = 34853$$

Step 3: Each integer of $C_0 = 18029, C_1 = 6030, C_2 = 17395, C_3 = 34853$ is converted into

$m_i = {C_i}^d \ mod\ 46189$,
we get, $m_0 = 32285, m_1 = 942, m_2 = 28913, m_3 = 20683$
Step 4: Calculate $R_i = m_i + (n \cdot k_i)$,
we have, $k_0 = 121, k_1 = 9306, k_2 = 1939723, k_3 = 239990633$
we get, $R_0 = 5621154, R_1 = 429835776, R_2 = 89593894560, R_3 = 11084927368320$
Step 5: The polynomial assuming $R_0 = 5621154, R_1 = 429835776, R_2 = 89593894560,$
$R_3 = 11084927368320$ as a coefficient

$$5621154 \cdot u^3 + 429835776 \cdot u^4 + 89593894560 \cdot u^5 + 11084927368320 \cdot u^6$$

Step 6: Apply inverse Sumudu Transform,

$$S^{-1}[\sum_{i=0}^{3} R_i u^{i+3}]$$

$$= S^{-1}[5621154 \cdot u^3 + 429835776 \cdot u^4 + 89593894560 \cdot u^5 + 11084927368320 \cdot u^6]$$
$$= (5621154)/3! \cdot t^3 + (429835776)4! \cdot t^4 + (89593894560)5! \cdot t^5 + (11084927368320)/6! \cdot t^6$$
$$= 936859 \cdot t^3 + 17909824 \cdot t^4 + 746615788 \cdot t^5 + 15395732456 \cdot t^6$$

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

The statistical analysis and frequency testing for this proposed method are presented. The graph of RSA algorithm and proposed method RSA-ST is shown here and also compared with each other. We used RSA, ST and proposed method RSA-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 RSA algorithm is the same, where the x-axis and y-axis represent plaintext and frequency level of ciphertext, respectively.

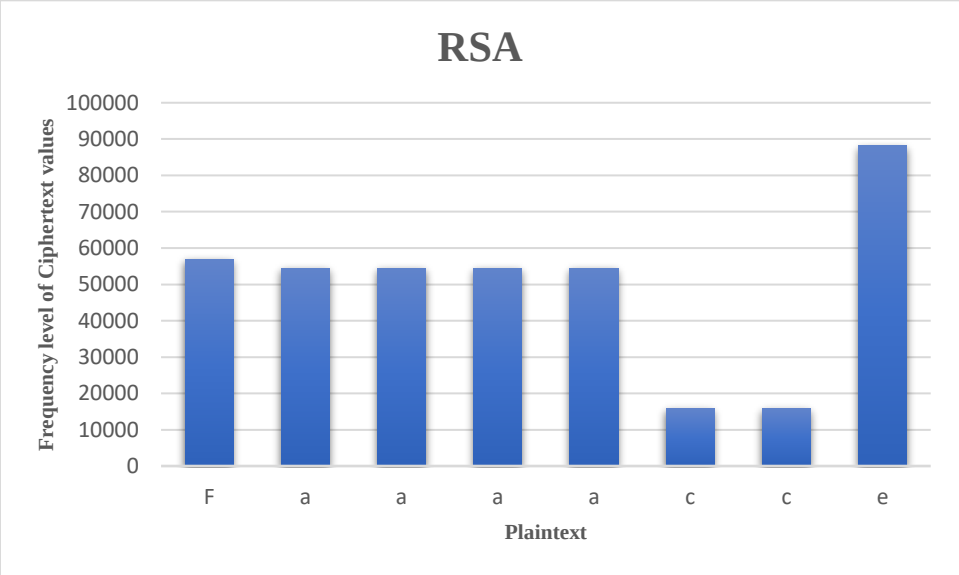

Fig. I: RSA algorithm ciphertext frequency distribution

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

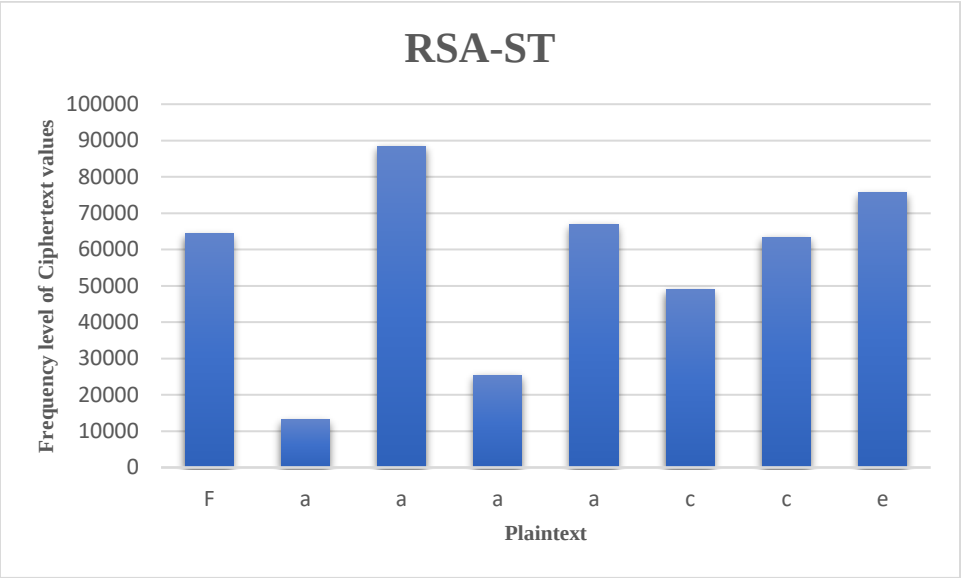

Fig. II: The proposed algorithm ciphertext frequency distribution

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

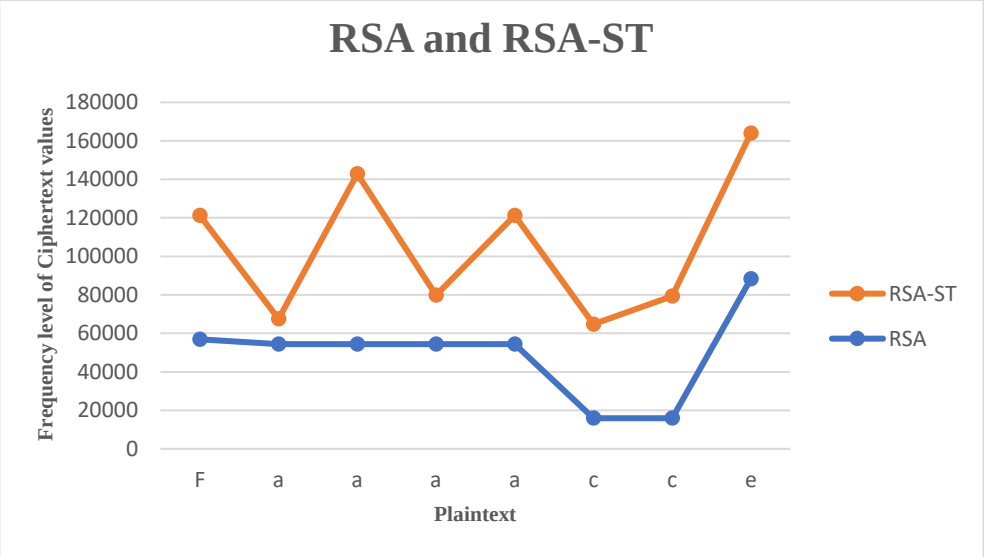

Fig. III: Ciphertext frequency distribution of RSA and RSA-ST

According to the frequency test, the proposed method RSA-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 and the correlation coefficient value of the proposed encryption method.

Table: The Correlation test from plaintext to ciphertext

Message	Method	Correlation
Arya23	RSA algorithm	0.45775859
	ST method	0.14308012
	RSA-ST proposed method	**-0.08051043**
CryPto	RSA algorithm	0.67704516
	ST method	-0.79330274
	RSA-ST proposed method	**0.47043211**
Cake	RSA algorithm	0.55760211
	ST method	-0.51297154
	RSA-ST proposed method	**0.32417235**

According to the correlation test, proposed method RSA-ST gives better result compare to RSA orST. Correlation coefficient values are closer to zero with this proposed method RSA-ST. However, for some data (message), RSAmay perform better than RSA-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. 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 Sumudu Transform of function providing four large prime numbers. It is impossible to break this method without knowing the private key. Therefore, this proposed method RSA-ST can provide more security of communication.

REFERENCES

[1]. Bodkhe D. S, Panchal S. K. (2015). "Use of Sumudu Transform in Cryptography", Bulletin of the Marathwada Mathematical society, 16/2: 1-6.

[2]. M. Tuncay GENÇOĞLU (2017). "Cryptanalysis Use of Sumudu Transform in Cryptography", researchgate/publication/319213093.

[3]. MuniruAderemiAsiru, "Further properties of the Sumudu transform and its applications", International Journal of Mathematical Education in Science and Technology 33 (2002).

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

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

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

[10]. 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.

[11]. Jeevitha S., Komala S., Silambarasi S., SusithaS.,Vanitha R. (2021). "An introduction of sumudu transform", Journal of Emerging Technologies and Innovative Research (JETIR), Volume 8, Issue 7, JETIR2107602, (ISSN-2349-5162).

[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]. 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.

[15]. 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.

[16]. 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.

[17]. 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.

[18]. 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).

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