IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

Encryption Scheme Involving Horizontal and Vertical Bit Rotation Simultaneously

Apurba Ghosh[1], Payel Mondal[2], Nilakash Mukherjee[3] and Niladri Kandar[4]

Faculty, Department of Basic Science and Humanities, Narula Institute of Technology, Kolkata, India[1,2]

Student, Department of Computer Science and Technology, Narula Institute of Technology, Kolkata, India[3,4]

Abstract: Cryptography is the practice of securing communication from third-party interception and manipulation that involves the use of mathematical algorithms to encrypt data, making it unreadable to anyone without the proper key. Encryption is the process of converting plaintext into ciphertext, while decryption is the reverse process of converting ciphertext back into plaintext. The use of cryptography is widespread in various fields, including finance, government, and military. The goal is to ensure the confidentiality, integrity, and authenticity of sensitive information. Cryptography is also used to protect digital signatures and passwords. There are two types of encryptions: symmetric key encryption and public key encryption. Symmetric key encryption uses a shared secret key to encrypt and decrypt data, while public key encryption uses a pair of keys, one public and one private, to encrypt and decrypt data. Both type of encryptions has their advantages and disadvantages, depending on the specific use case. The strength of encryption depends on the key size and the complexity of the algorithm used. In this paper we are proposing an algorithm on encryption and decryption to convert a plain text into a ciphertext and vice versa. The method suggests to divide the text in blocks and each block are of 8 bytes. Then each letter of a block will be converted into their ASCII. Then structure the ASCII in an 8 x 8 matrix form. After that, the matrix will be sub-divided into 4 matrices and the 4 sub matrices will be gone through vertical and horizontal bit rotation. As computers become more powerful, it is essential to regularly update encryption methods to ensure the security of the encrypted data. Overall, cryptography and encryption-decryption play a crucial role in securing sensitive information in today's digital world.

Keywords: Quantum cryptography, Vertical bit rotation, Horizontal bit rotation, Ceiling

I. INTRODUCTION

In an increasingly interconnected digital world, ensuring the security and confidentiality of sensitive information has become a paramount concern. Cryptography, the art and science of secure communication, has played a pivotal role in safeguarding data from prying eyes for centuries. From its early origins in classical ciphers to its revolutionary applications in modern computing systems, cryptography has constantly evolved in response to the ever-growing threats posed by malicious actors and advancing technologies.

The paper will navigate through the foundational principles of encryption and decryption, highlighting the challenges posed by key management, algorithm vulnerabilities, and the impending arrival of quantum computing. As classical cryptographic techniques encounter new vulnerabilities and limitations, the emergence of quantum cryptography promises to reshape the security landscape by leveraging the principles of quantum mechanics. Through a comprehensive analysis of cryptographic techniques, their strengths, weaknesses, and potential vulnerabilities, this research aims to contribute to the broader understanding of how cryptography has evolved and adapted to meet the demands of an interconnected world.[1] By exploring the transitions from classical to quantum cryptography, we aim to shed light on the future directions of secure communication, providing insights that will be invaluable in designing robust cryptographic systems for the digital age.[2-5]

II. PROPOSED TECHNIQUE

Generating Key: The key is generated using random number generators of the size no less than 128 bits. Then the key will be divided into two halves. The sum of the digits of the first half will determine that if it is even then principal diagonal will be rotated of the matrix. Else, the anti-diagonal will be rotated of the matrix. The sum of the digits of the second half will determine that if it is even then horizontal bit rotation will be done else, vertical bit rotation will be done.

Encryption Technique: The encryption will be done in two steps.

(i) Divide plain text into blocks: The plain text is divided into blocks of 8 bytes. The formula to calculate the number of blocks required for text is ‘ceiling (length (TEXT)/8)’.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

PLAIN_TEXT = "ENCRYPTION"
BLOCK_1 = "ENCRYPTI"
BLOCK_2 = "ON_____"

If the last block does not match the selected block size, then padding "_" can be added to fill the block.

(ii) Converting each byte in to their ASCII in and forming a [8 x 8] matrix for each block:

E	0	1	0	0	0	1	0	1
N	0	1	0	0	1	1	1	0
C	0	1	0	0	0	0	1	1
R	0	1	0	1	0	0	1	0
Y	0	1	0	1	1	0	0	1
P	0	1	0	1	0	0	0	0
T	0	1	0	1	0	1	0	0
I	0	1	0	0	1	0	0	1

O	0	1	0	0	1	1	1	1
N	0	1	0	0	1	1	1	0
-	0	0	1	0	0	0	0	0
-	0	0	1	0	0	0	0	0
-	0	0	1	0	0	0	0	0
-	0	0	1	0	0	0	0	0
-	0	0	1	0	0	0	0	0
-	0	0	1	0	0	0	0	0

(iii) Divide the matrices into sub-matrices:

E	0	1	0	0
N	0	1	0	0
C	0	1	0	0
R	0	1	0	1

0	1	0	1
1	1	1	0
0	0	1	1
0	0	1	0

O	0	1	0	0
N	0	1	0	0
-	0	0	1	0
-	0	0	1	0

1	1	1	1
1	1	1	0
0	0	0	0
0	0	0	0

BLOCK 1 BLOCK 2

Y	0	1	0	1
P	0	1	0	1
T	0	1	0	1
I	0	1	0	0

1	0	0	1
0	0	0	0
0	1	0	0
1	0	0	1

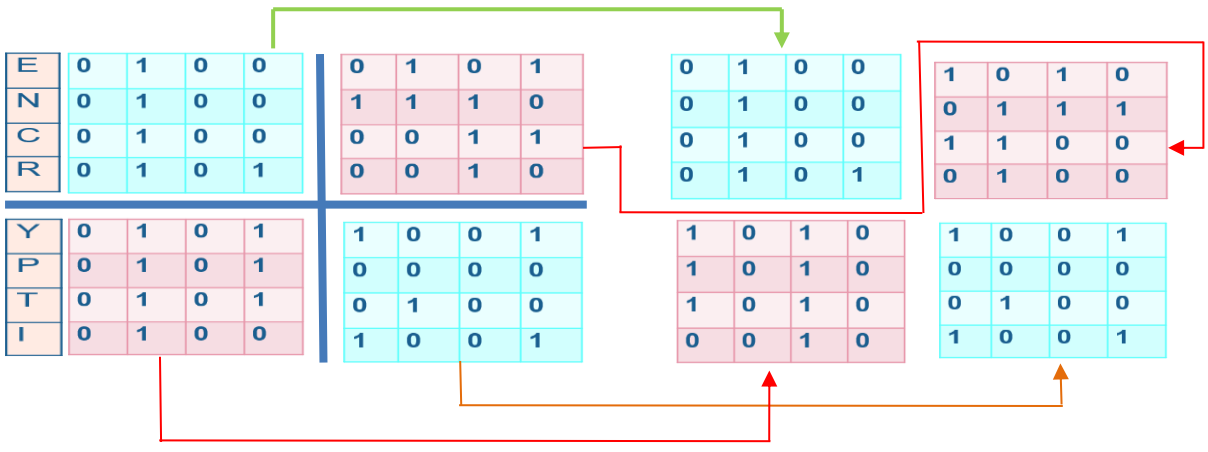
-	0	0	1	0
-	0	0	1	0
-	0	0	1	0
-	0	0	1	0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

(iv) Now as per **key mechanism:**

A key is generated 854639 (say). Now it will be divided into two halves, 1st half is 854 and the 2nd half is 639. The sum of the digits of the first half is 17 and the sum of 2nd half is 18. Since 1st part is odd, the bit rotation will perform on the anti-diagonal sub-matrices and 2nd part is even so, horizontal bit rotation will take place.

BLOCK 1



IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

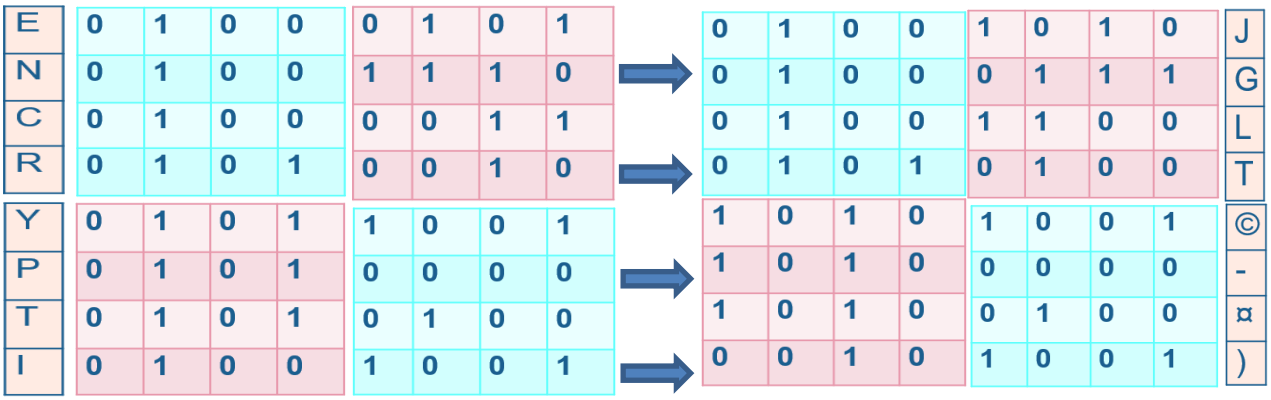
International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

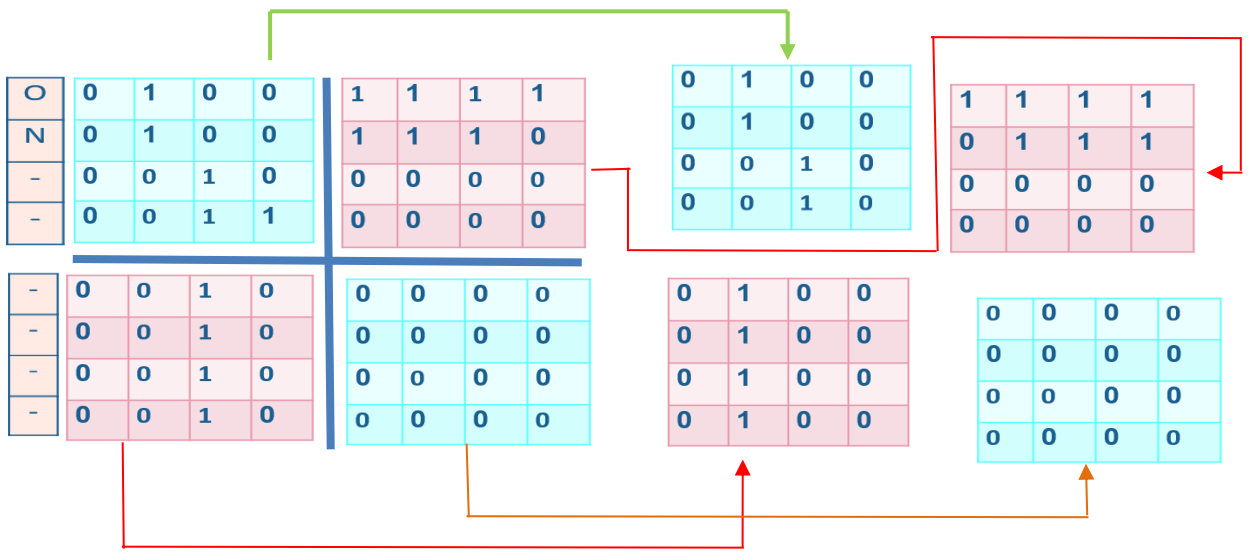
Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

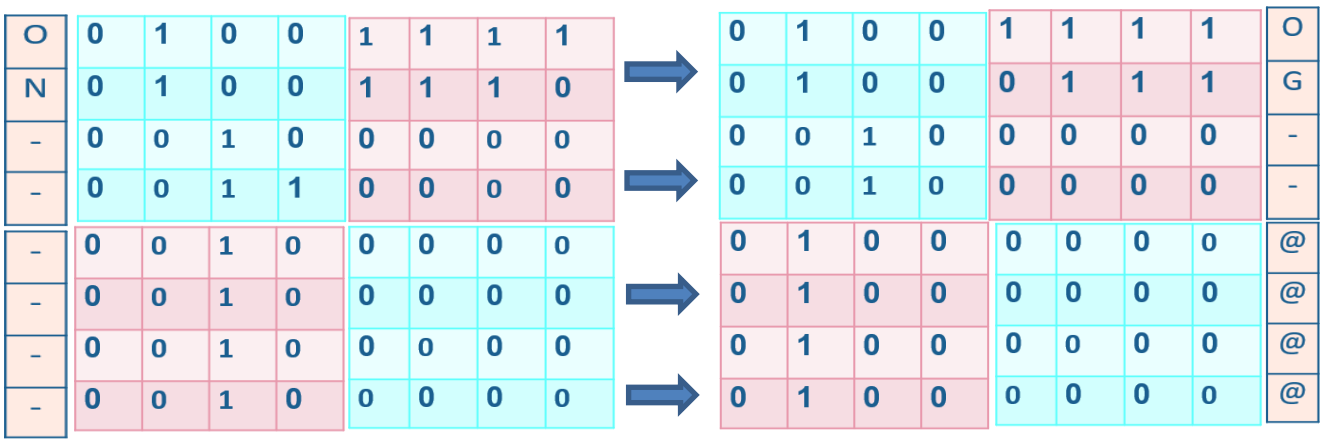
Here the diagonal and the anti-diagonal bit rotations are taking place as per the key mechanism. Now, after rotating the blocks we will concatenate the blocks and as well as the matrices to get the encrypted text.



BLOCK 2



Again, concatenation of the 4 matrices will provide the required cipher similarly.



So, after going through the process we get the encrypted text of "***ENCRYPTION***" as "J ***G L T*** © - ¤***)***".

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

***C.* Decryption Technique:**

The decryption will be done in two steps.

(i) Divide cipher text into blocks: The cipher text is divided into blocks of 8 bytes. The formula to calculate the number of blocks required for text is 'ceiling (length (TEXT)/8)'.

CIPHER_TEXT = "ENCRYPTION"
BLOCK_1 = "JGLT©-¤)"
BLOCK_2 = "OG--@@@@"

If the last block does not match the selected block size, then padding "_" can be added to fill the block.

(ii) Converting each byte in to their ASCII in and forming a [8 x 8] matrix for each block:

J	0	1	0	0	1	0	1	0
G	0	1	0	0	0	1	1	1
L	0	1	0	0	1	1	0	0
T	0	1	0	1	0	1	0	0
©	1	0	1	0	1	0	0	1
-	1	0	1	0	0	0	0	0
¤	1	0	1	0	0	1	0	0
)	0	0	1	0	1	0	0	1

O	0	1	0	0	1	1	1	1
G	0	1	0	0	0	1	1	0
-	0	0	1	0	0	0	0	0
-	0	0	1	0	0	0	0	0
@	0	1	0	0	0	0	0	0
@	0	1	0	0	0	0	0	0
@	0	1	0	0	0	0	0	0
@	0	1	0	0	0	0	0	0

(iii) Divide the matrices into sub-matrices:

BLOCK 1

J	0	1	0	0
G	0	1	0	0
L	0	1	0	0
T	0	1	0	1

1	0	1	0
0	1	1	1
1	1	0	0
0	1	0	0

©	0	1	0	0
-	0	1	0	0
¤	0	1	0	0
)	0	1	0	1

1	0	0	1
0	0	1	0
0	1	0	0
1	0	0	1

BLOCK 2

O	0	1	0	0
G	0	1	0	0
-	0	0	1	0
-	0	0	1	0

1	1	1	1
0	1	1	0
0	0	0	0
0	0	0	0

@	0	1	0	0
@	0	1	0	0
@	0	1	0	0
@	0	1	0	0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

(iv) Now as per key mechanism:

A key is generated 854639 (say). Now it will be divided into two halves, 1st half is 854 and the 2nd half is 639.

The sum of the digits of the first half is 17 and the sum of 2nd half is 18. Since 1st part is odd, the bit rotation will perform on the anti-diagonal sub-matrices and 2nd part is even so, horizontal bit rotation will take place.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

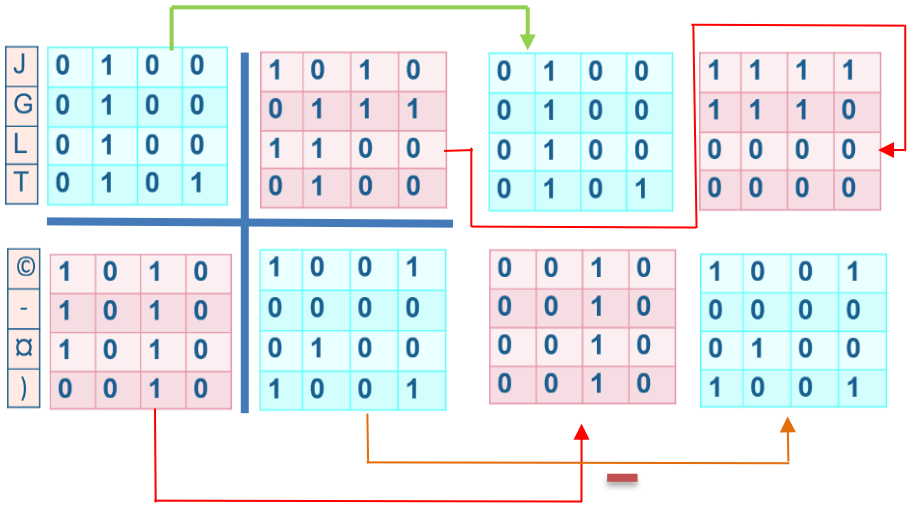
International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

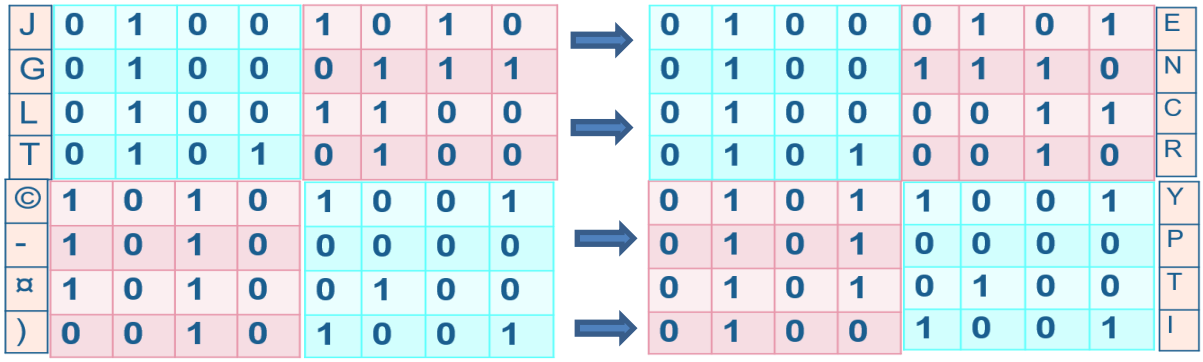
Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

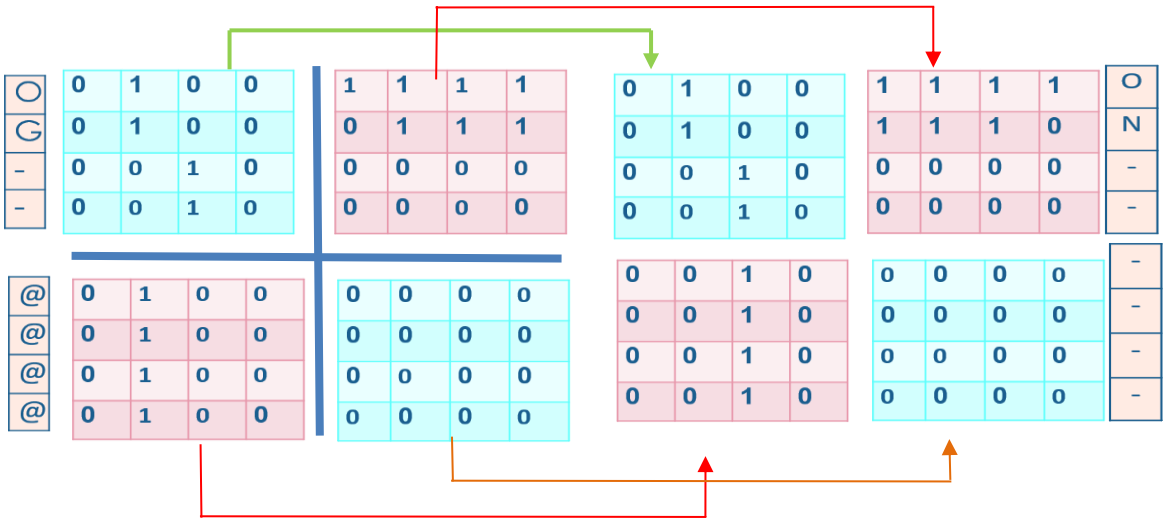
BLOCK 1



Here the diagonal and the anti-diagonal bit rotations are taking place as per the key mechanism. Now, after rotating the blocks we will concatenate the blocks and as well as the matrices to get the decrypted text.



BLOCK 2



IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

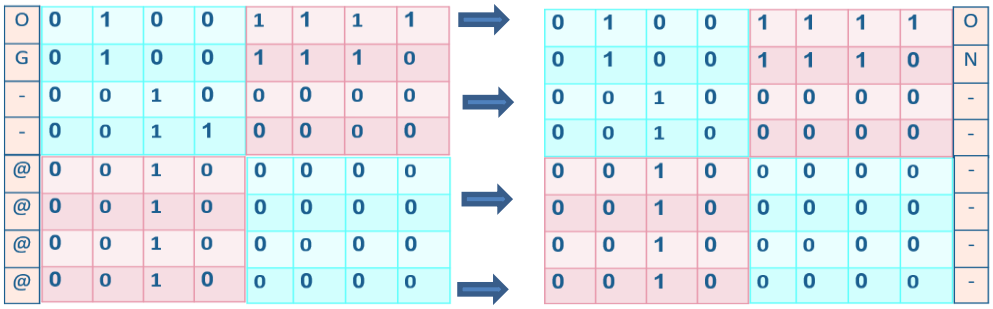
International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

Again, concatenation of the 4 matrices will provide the required cipher similarly



So, after going through the process we get the decrypted text of **"J G L T © - ¤ OG--@@@)"** as "**ENCRYPTION".**

III. PERFORMANCE ANALYSIS

This section analyses the proposed algorithm's time complexity and compares it with AES and RSA encryptions system. AES Encryption is meant for fast encryption and decryption, it could encrypt hundreds of megabytes per second. [6-10] However, the speed varies with different versions of AES. RSA is public key encryption system i.e. the cryptosystem uses pair of keys for encryption and decryption. RSA has a specific limit to how much it can encrypt in one go; it varies with different key sizes.

Encryption and decryption comparison

TABLE 1 ENCRYPTION COMPARISION WITH .TXT FILE

File name (.txt)	Size (Bytes)	Encryption Time (Seconds)		
		RSA	AES	Proposed Algo.
file_1.txt	262144	0.828	0.558	6.245
file_2.txt	524288	3.182	0.604	11.352
file_3.txt	786432	7.202	0.625	19.457
file_4.txt	1048576	13.502	0.65	23.736
file_5.txt	1310720	20.09	0.678	28.164

TABLE 2 DENCRYPTION COMPARISION WITH .TXT FILES

File name (.txt)	Size (Bytes)	Encryption Time (Seconds)		
		RSA	AES	Proposed Algo.
file_1.txt	262144	0.91	0.359	7.673
file_2.txt	524288	3.948	0.421	12.541
file_3.txt	786432	5.494	0.512	19.857
file_4.txt	1048576	10.469	0.58	24.87
file_5.txt	1310720	16.44	0.624	33.659

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

IV. CONCLUSION

The key point for the proposed technique is that it has similar security as compared to RSA and AES. Even though it has taken longer time in encryption and decryption for large file sizes, the main usability for this encryption would be to encrypt keys for other encryption system or can be used to encrypt small amount of data for cell phones, RFID cards, Smart tags etc. It has a high chi square value which shows that the encryption technique is secure for use.

REFERENCES

[1]. Gupta A. and Walia N. K. (2014). Cryptography Algorithms: A Review. International Journal of Engineering Development and Research, 2 (2).
[2]. Davies and Donald (1997). A brief history of cryptography. Information Security Technical Report. 2. 14-17.
[3]. Wei N. and Wei W. (2013). Analysis and Research of the RSA Algorithm. Information Technology Journal, 12 (9), 1818-1824.
[4]. Som S. and Banerjee M. (2013). Cryptographic technique by square matrix and single point crossover on binary field. 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, United Arab Emirates.
[5]. Devika G. and Shankar K. (2017). A Modified Symmetric Key Cryptography Method for Secure Data Transmission. International Journal of Pure and Applied Mathematics.
[6]. Noorunnisa, Nahri, Siddiqui, Rahat (2016). Review on Honey Encryption Technique. International Journal of Science and Research (IJSR), 5, 1683-1686.
[7]. Danasingh, Antony. A (2016). Performance Analysis of Data Encryption Algorithms for Secure Data Transmission. International Journal for Science and Advance Research in Technology, 2, 388-390.
[8]. Aanjanadevi S., Palanisamy V. and Aanjankumar S. (2019). An Improved Method for Generating Biometric-Cryptographic System from Face Feature, 10.1109/ICOEI.2019.8862741, 1076-1079.
[9]. Palanisamy V. and Jeneba Mary A. (2011 April). Hybrid cryptography by the Implementation of RSA and AES. International Journal of Current Research, 3 (4), 241-244.
[10]. Som S., Chatergee N. S. and Mandal J. K..(2011). Key based bit level genetic cryptographic technique (KBGCT). IEEE, Melaka, Malaysia.