e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

A STUDY ON MODIFIED RSA ALGORITHM IN NETWORK SECURITY

Abhishek*1, Dr. Vandana*2

*1Department Of Computer Science, KLSM Mahvidyalaya, CCSU, Meerut, India.

*2Department Of Computer Application, SCRIET, CCSU, Meerut, India.

ABSTRACT

This research paper aims to endeavours modified method of RSA algorithm so the more secure RSA algorithm can be developed. RSA algorithm provides the security service to every user who is connected through the network. Many cryptographic algorithms are used to exchange the information over network. RSA cryptosystem algorithm is widely used cryptographic algorithm in network security but it has problem of integer's factorisation for small numbers. Researchers have proposed many modifications to improve the security of traditional RSA. In this research various modifications are presented and compared to figure out new approaches of RSA cryptosystem, which try to improve the security and speed up the time of key generation encryption and decryption process.

Keywords: RSA, Algorithm, Security, Encryption, Decryption.

I. INTRODUCTION

In today's world, network security is a challenging subject. Many techniques have been designed to safeguard prevent from attacks. Millions of people are connected to the network and its major objective is to secure the data and information until it reaches its destination on time. Network security also ensure confidentiality, integrity, availability, access control, authorization, and nonrepudiation. [1]

Cryptography is one of the best solutions to communicate on the network. Cryptography is a Greek word that means 'hiding information'. Cryptography ensures the secrecy of the message. It is a guideline method for secure information transmission, where information in encrypted form is included with or without a key. The message is encrypted by an algorithm and key from the sender side and encrypted text, known as cipher-text is sent to the receiver side then this cipher-text is decrypted by the receiver key and gets the original message back.

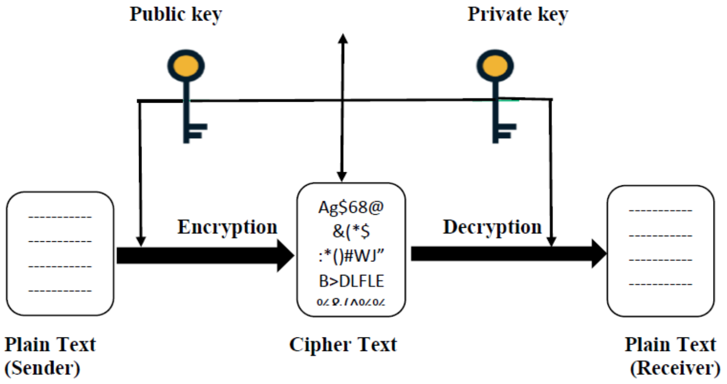

Figure 1: Public-Key Cryptography model

The symmetric-key cryptography and the asymmetric-key cryptography both are based on a public and private key concept. In symmetric-key cryptography, only one key i.e. public-key is used for encryption and decryption on the sender and receiver's side so it can be easily accessed by the third party, which means it is not a secure method for data transmission. DES, AES, IDEA, Blowfish are the type of symmetric-key cryptography. In asymmetric key cryptography, two keys are used i.e. public key and private key, on the sender side data is encrypted by the receiver public key and decrypt only by private-key of the receiver so it is more secure method for data transmission because different keys are used for encryption and decryption. RSA, Elliptic curve algorithms are the type of asymmetric key cryptography.

Asymmetric-key or public-key cryptography is one of the valuation solutions for sending information in a secure channel. RSA algorithm is one of them

RSA Cryptosystem

RSA algorithm is the most popular cryptography algorithm in network security. It was invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1977 at MIT [2]. It is widely used in network security. In this two big prime numbers are used. There are two major open problems of RSA i.e. Integer Factorization problem and the RSA problem [10] i.e. finding the Nth root. N is the product of two prime numbers. RSA uses two keys, public and private keys. Public-key is used for only encryption and private key is used for decryption. According to the number theory, it is easy to compute the product of two large numbers but factorization is hard. In RSA security depends on the factor of the large numbers. The key size in the RSA algorithm is 2048 to 4096 [10] which is difficult to factorize. Decryption in RSA algorithm based on d and N, d represent decryption key. The Time complexity of RSA is O (n2). To improve the security is of the traditional RSA algorithm, many modifications are being proposed by researchers.

There are three processes of the RSA algorithm

A. Key generation.
B. Encryption.
C. Decryption.

A. Key generation

- Generate two large random prime numbers p and q. ∈ gcd (p, q) = 1.
- Compute n=p * q.
- Compute Euler's totient function Ø(n) = (p-1)*(q-1).
- Choose public key integer e, where 1< e < Ø(n) ∈ gcd(Ø(n), e) = 1.
- Compute private key integer d, d=e-1mod Ø(n).
- Public key is (e, n) and private-key is (d, n)

B. Encryption

- Public key (e, n), let cipher-text as c, message as m.
- Encrypt message in cipher-text c = me mode n.
- A sends the cipher-text c to B.

C. Decryption

- Private Key (d, n).
- Decrypt cipher-text m = cd mod n.
- B can read the original message.

II. RELATED WORK

A. Select Additional 'n' prime number:

In this method, Urbana et al. [4] suggested an improvement to enhance the security of the RSA algorithm using 'n' prime number instead of choosing two prime numbers. It is difficult to find the factor of the product of multiple prime numbers than the product of two prime number, which increases the efficiency of the algorithm and makes it more secure.

B. Hybrid approach using RSA and Diffie-Hellman key exchange:

This is the combined concept [5] of RSA and Diffie-Hellman key exchange algorithms. Diffie-Hellman algorithm is used to exchange secret keys between both parties. In this combined algorithm, S. Gupta and J. Sharma in 'A Hybrid Encryption algorithm based on RSA and Diffie-Hellman', generated a private key (d) and public key (e) using the RSA algorithm and after generating keys e and d, apply the Diffie-Hellman algorithm, and then generated a secret key. Using this secret key, the message is encrypted using XOR operation between secret key and message and for decryption also apply XOR operation between secret key and cipher-text. Secret keys are the same for both the sender side and receiver sides. This combined algorithm will be easy for the user to send and receive the messages and files, which makes it more confidential.

C. Hybrid approach using Diffie-Hellman key exchange and RSA:

This is another combine concept of Diffie Hellman and RSA. Bhattachargee et al. [6] introduced the approach that uses the session key of the Diffie Hellman algorithm in the RSA cryptosystem, to apply the multiplication of session key with prime numbers, and replace that multiplied value with RSA 'N' variable with an encryption key only. This approach will not be prone to mathematical factorization attacks like RSA. This technique of RSA cryptosystem makes it more difficult to factorization attacks.

D. Improved RSA

Jahan et al. [7] did a change in the public key of the RSA algorithm. It provides little high security as compared to the traditional algorithm, it also provides better performance than traditional RSA cryptosystem algorithms. In this method, an encryption key is broken into two numbers. So in IRSA public key is sent twice separately. The time of key generation, encryption and decryption is more than RSA because there is additional x and y operation. This algorithm uses two public keys instead of one public key, which makes the algorithm more effective in terms of security, less vulnerability hence improves the reliability for brute force attack.

E. Modified RSA Algorithm

Dhakar et al. [8] introduced a Modified RSA encryption algorithm (MREA), which contains homomorphic properties. It increases the complexity of factorization when module length increases. MREA has another multiplicative module, it uses two module n and µ. where calculating the inverse multiplicative for both modules, increases the security to calculate the private key. Increased length of the modules provides better security but decrease the speed of key generation, encryption and decryption. MREA provides dual security but the time of execution is slower than RSA. The time complexity of MREA is O (n + n3).

F. RSA algorithm with speed up process

Nagar and Alshamma [9] create a new method of keys exchange, which speeds up the key exchange process between sender and receiver with RSA handshaking protocol. They used a database engine to store RSA modules, public and private keys. It provides four security level, each level has its own database, and each database has many sets. Levels are identified according to the length of modules. The database stores the already generated RSA modules P, Q, N, and Ø(N) and public key e and private key d. This protocol is responsible for the creation and updation of the identical offline database of key generation, manage the gateway, and control the security levels. The author uses index exchange method. This method is fast and more secure because the only id is exchanged from the pre-generated offline database, using the id, it will be hard to get the keys and N. This method is 2.5 times faster than normal RSA keys generation because it reduces the calculation time of key generation.

III. ANALYSIS OF ALGORITHM

In this paper we have compared the result of various algorithm presented here, using python libraries to compare the time taken by different algorithms. For the sake of c, we used 16-bit modules size and 16-bit message size.

Table: Comparison table of algorithms

S. No.	Algorithm	Key Generation Time(µsecond)	Encryption Time (µsecond)	Decryption Time (µsecond)	Total Time (µsecond)
1.	RSA	997	999	1998	3994
2.	N Prime numbers RSA	998	1998	13992	16988
3.	RSA-Diffie key exchange	1000	998	999	2997
4.	Diffie key exchange-RSA	999	1000	999	2998
5.	IRSA	900	995	2000	3895
6.	MREA	2998	40174	48967	92139

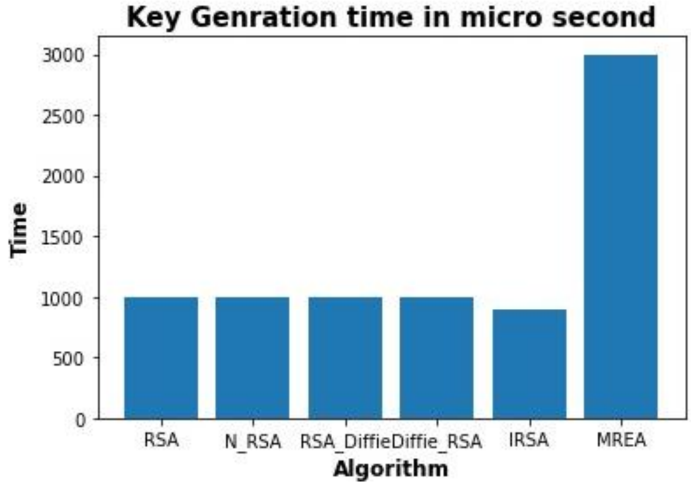

Figure 2: Key Generation time comparison of different algorithms

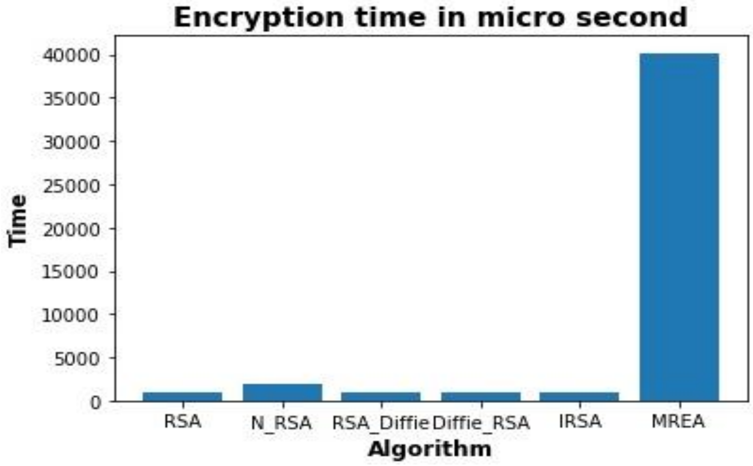

Figure 3: Encryption time comparison of different algorithms

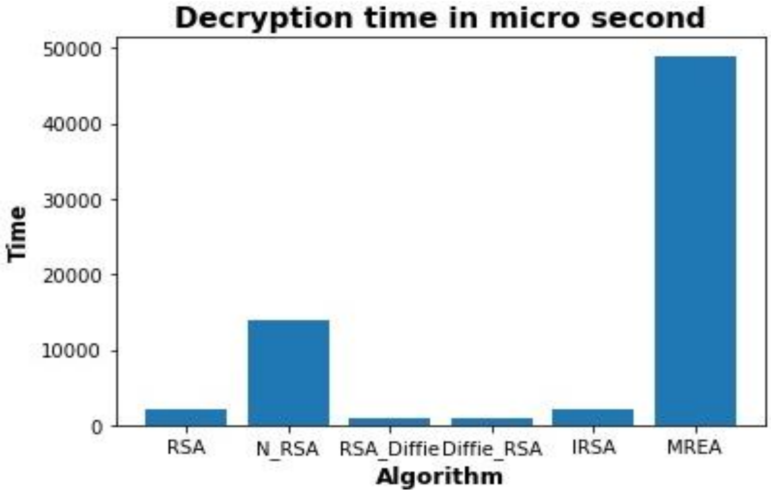

Figure 4: Decryption time comparison of different algorithm

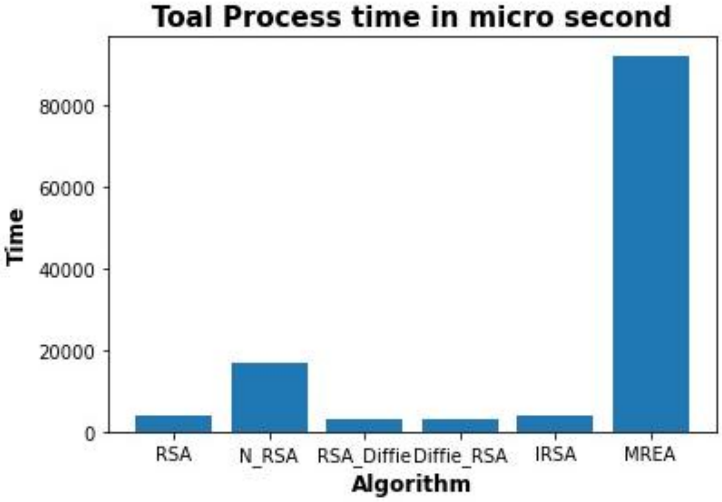

Figure 5: Total process time comparison of different algorithms

IV. CONCLUSION

In the study of the normal RSA algorithm, the question is developed whether it is secure or not? Nowadays computers are available with the high processor, and fast execution. Quantum computer is one of them. The high processing power of quantum computers can easily compute thousands of bits of numbers. According to the Riemann hypothesis, if the frequency of prime number is found, then it will be easy to find the factor of multiplicative prime numbers. So, a more secure RSA algorithm is required to be developed. In this paper, some modified methods of the RSA algorithms are discussed. Researchers tried to performed a more secure RSA algorithm thus, the study of this paper figures out, that every day new approaches are developed which try to improve the security and speed up the time of key generation, encryption and decryption process.

V. REFERENCES

[1] W. Stalling, “Cryptography and network security: principles and practice”, Pearson, fifth edition, 2011 ISBN 13: 978-0-13-609704-4.

[2] R.L. Rivest, A. Shamir, and L. Adleman, ‘A Method for Obtaining Digital signatures and Public-Key Cryptosystems,’ Communications of the ACM, Feb. 1978 vol. 21(2) pp. 120- 126’.

[3] B. R. Ambedkar, S.S. Bedi, ‘A New Factorization Method to Factorize RSA Public Key Encryption ’, International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, Nov 2011.

[4] B.P. Urbana Ivy, P. Mandiwa, M. Kumar, ‘A Modified RSA Cryptosystem based on ‘n’ Prime Number’, International Journal of Engineering And Computer Science ISSN: 2319-7242 Vol. 1 Issue 2 Nov 2012 pp. 63-66.

[5] S. Gupta and J. Sharma, ‘A Hybrid Encryption Algorithm based on RSA and Diffie- Hellman’, 2012 IEEE International Conference on Computational Intelligence and Computing Research.

[6] A. Bhattacharjee, C. Khaskel, D. Basu, D. R. Vincent P.M., ‘Hybrid Security Approach By Combining Diffie-Hellman and RSA Algorithm’, International Journal of Pharmacy and Technology Dec. 2016 Vol. 8 Issue No. 4 pp. 26560-26567.

[7] Israt Jahan, Mohammad Asif, Liton Jude Rozario, ‘Improved RSA Cryptosystem based on the Study of Number Theory and Public-key Cryptosystems.’ American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN: 2320-0936 vol.-4 Issue-1 pp. 143-149.

[8] R. S. Dhakar A. K. Gupta and P. Sharma, ‘Modified RSA encryption algorithm (MREA)’, 2012 2nd International Conference on Advanced Computing and Communication Technologies IEEE. pp. 426-429.

[9] Sami A. Nagar and Saad Alshamma. ‘High Speed Implementation of RSA Algorithm with Modified Keys Exchange.’ Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on IEEE.

[10] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[11] https://en.wikipedia.org/wiki/shor%27s_algorithm.