# A Comprehensive Study on Various Modifications in RSA Algorithm

[1]Gaurav R. Patel, [2]Prof. Krunal Panchal, [3]Sarthak R. Patel
[1,3]PG Scholar, [2]Assistant professor
LJIET, Ahmedabad
[1]guravpatel9092@gmail.com, [2]krunaljpanchal@gmail.com, [3]patelsarthakr@gmail.com

***Abstract:*** **Cryptography is derived from a Greek word which means the art of protecting information by converting it into an unreadable format. In order to prevent some unwanted users or people to get access to the data cryptography is needed. This paper surveys various modifications approaches applied on standard RSA algorithm in order to enhance it. RSA provide more security as compare to other algorithm but the main disadvantage of RSA is its computation time, so many researchers applied various techniques to enhance the speed of an RSA algorithm by applying various logic and also apply some techniques which can be used for data integrity. This paper does the detailed study about such techniques and represents the summarized results.**

***Key Terms: RSA, Diffie-Hellman,, Cryptography, Cryptosystem, private-key, public-key.***

## I. INTRODUCTION

Cryptography is a technique to hide the data over communication channel. It is an art to hide the data to strangers. As the technology grows day by day the need of data security over communication channel is increased to high extent. For securing the knowledge cryptography is use.Symmetric key (also known as secrete-key cryptography) uses the only one key for both encryption and decryption.

Asymmetric key (also known as public key encryption) uses two different keys to encryption and decryption of the message. The public key is made publicly available and can be used to encrypt messages. The private key is kept secret and can be used to decrypt received messages. RSA is asymmetric key encryption algorithm [9]. RSA uses two different keys for encryption and decryption leading to secure transmission of messages. RSA algorithm involves three different phases [6]:

**Phase 1: Key Generation**

RSA involves two keys public key and private key. For encryption we use Public key and for decryption we use private key of message. The key generation takes places as follows [2]:

**(a)** Choose three distinct prime numbers P and Q

**(b)** Find N such that N= P*Q,

**(c)** Find the Phi of N, $\emptyset(N)$= (P-1)*(Q-1).

**(d)** Choose an E such that 1 < E < $\emptyset(N)$ and such that E and $\emptyset(N)$ share no Divisors other than 1 [E and $\emptyset(N)$ are relatively prime]. E is kept as the public key exponent.

**(e)** Determine D which satisfies the congruence relation.

E*D = 1 (mod $\emptyset(N)$).

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

**Public Key: (E, N)**

**Private Key: (D, N)**

**Phase 2: Encryption**

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure environment. The process of encryption requires two things- a key and an encryption algorithm. Encryption takes place at the sender side. C = M ^ E mod (N)

**Phase 3: Decryption**

It is a process of converting Cipher Text into Plain Text. This reverse process of encryption is called as Decryption. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. M = C ^ D mod (N)

## II. RELATED WORK

**Alaa Hussein, Al-Hamami and Ibrahem Abdallah Aldariseh** proposed enhancing the RSA algorithm; in this RSA algorithm they used additional third prime number in the composition of the private and public key. Because of additional prime number the factoring complexity of variable (n) is also increase. [2]

**Aayush Chhabra and Srushti Mathur** introduces approach which provides more security than RSA algorithm, which is used for encryption and digital signatures in public key cryptography. This approach reduces the need to transfer *n*, the multiplication of two random big prime numbers. Because of large prime numbers it becomes difficult for the hacker to guess the factors of *n* so the encrypted message will be safe from the attacker. This approach provides a more secure path for communication through public key cryptography. [3]

**Sun, Wu, Ting, and Hinek** proposed new method of an RSA in which the key generation algorithms output is two distinct RSA key pairs. The public key and private key exponents are same. This family of variants is known as Dual RSA and it can be used for two instances of RSA with the advantage of reducing the data storage requirements of the keys. Two applications for Dual RSA, blind digital signatures and authentication are proposed. As compared to normal RSA, the security boundary should be raised when we are using Dual RSA to the types of Small-d, Small-e, and Rebalanced-RSA. [4]

**Wang Rui, Chen Ju, Duan Guangwen** constructed a k-RSA algorithm in which the idea of RSA algorithm and kth power residue theory is combined. This algorithm not only inherits the advantage of RSA, whose security is depends on the factoring of large numbers and finding of discrete logarithms, but also has high flexibility of parameters. This approach improved security and also achieve a balance between speed and space. At the same time, it can realize functions like hierarchical system management and secret sharing. The result shows that, in the case of e equality, d is small in k-RSA algorithm. This new algorithm can reduce the power computation in decryption. [6]

**Shilpi Gupta and Jaya** introduces new concept using two most important algorithms RSA and Diffie-Hellman. This approach will provide more communication security. The RSA algorithm can be used for public key encryption and digital signature. Diffie Hallman algorithm is used as key exchange method that allows two parties that have no proper knowledge to each other to jointly share a secret key. In this approach the RSA keys were taken as input for Diffie Hellman. The required keys are generated using RSA algorithm. The Diffie Hallman is used for generating more secure cipher text. [7]

**Vishal Garg and Rishu** introduces new approach which provides harder encryption with enhanced public key encryption protocol for security. The work provide some solution for better encryption algorithms and try to provide better security to email services and to other web services. This approach is helpful for sending secure email or any kind of message on internet. This approach provides better security to any network. We can increase the security of Diffie-Hellman encryption algorithm by adding more security codes in current algorithm. [8]

**Gaurav Shrivastava** proposes a new approach to enhance the security of cryptosystem. The Data Encryption Standard (DES) is the most common Secret Key Cryptography scheme. DES so far has been stronger than other cryptosystems in the security.DES may be attacked by parallel processing. If you want to protect DES encryption system strong you need to follow this approach .In approach they will use Triple DES Three Times with RSA Algorithm. This will provide 504 bit key length. This new algorithm enhance the security level but also responsible for increase in the file size. [9]

**Khushdeep Kaur, Er. Seema** proposed a new approach by combining DSA, RSA and MD5 algorithm as a hybrid link for wireless devices. This is very efficient and secure hybrid algorithm for providing security to mobile nodes. They tested their proposed algorithm with different scenarios and it is providing better response time, less network delay and best throughput. The hybrid algorithm provides better results than other algorithms. This algorithm can be implemented to mobile nodes for security purposes. Also our research shows that it is helping in efficient routing of packet with much less load on servers. [10]

**Harsh Chitrala, Dhananjay Pugila, Salpesh Lunawat, P.M.Durai Raj Vincent** introduce algorithm which is similar to RSA algorithm but there is some modification in existing RSA algorithm.. In this approach there are two values of N: N1 and N2. The value of N1 is determined using four variables. This process creates difficulties to factorize value of N1. For encryption process they used N1 and for decryption N2 is used. This modification increases the security of RSA algorithm. If the hacker manages to factorize N1, it will be very complicate to determine the prime numbers from factors. This modification increases the security of the cryptosystem. This approach is more secure than RSA algorithm. The main advantage of this algorithm is that, the time taken for brute-force attack is more compared to RSA algorithm. [11]

## III. Conclusion

In this paper, it has been surveyed that the existing works on the RSA algorithm. Those techniques are studied and analyzed deeply to promote the performance of RSA algorithm and also to ensure the security of information. All the techniques are useful to speed up the RSA algorithm and for better security. Each technique is unique, which might be used for different applications. Everyday new approach is evolving hence fast and secure RSA algorithm always work out with high rate of security.

## References

[1] William Stallings, “Cryptography and Network Security”, ISBN 81-7758-011-6, Pearson Education, Third Edition
[2] Al-Hamami, A. H., & Aldariseh, I. A. (2012, November). Enhanced Method for RSA Cryptosystem Algorithm. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp. 402-408). IEEE.
[3] Chhabra, A., & Mathur, S. (2011, October). Modified RSA Algorithm: A Secure Approach. In Computational Intelligence and Communication Networks (CICN), 2011 International Conference on (pp. 545-548). IEEE.
[4] Sun, Hung-Min, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek. "Dual RSA and its security analysis." Information Theory, IEEE Transactions on 53, no. 8 (2007): 2922-2933.
[5] Dhakar, R. S., Gupta, A. K., & Sharma, P. (2012, January). Modified RSA Encryption Algorithm (MREA). In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on (pp. 426-429). IEEE.
[6] Wang Rui; Chen Ju; Duan Guangwen, "A k-RSA algorithm," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.21,24, 27-29 May 2011
[7] Gupta, S., & Sharma, J. A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman.
[8] Garg, V., & Rishu, R. (2012). Improved Diffie-Hellman Algorithm for Network Security Enhancement. International Journal of Computer Technology and Applications, 3(4).
[9] TT II, C. C. H. H. A. A. R. R., and CCLL EE. "Analysis Improved Cryptosystem Using DES with RSA
[10] Kaur, Khushdeep, and Er Seema. "Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices." International Journal of Engineering Research and Applications (IJERA) 2.5 (2012): 914-917

[11] Pugila, Dhananjay, Harsh Chitrala, Salpesh Lunawat, and PM Durai Raj Vincent. "AN EFFICEIENT ENCRPYTION ALGORITHM BASED ON PUBLIC KEY CRYPTOGRAPHY." International Journal of Engineering and Technology (2013).

[12] Ambedkar, B. R., Gupta, A., Gautam, P., & Bedi, S. S. (2011, June). An Efficient Method to Factorize the RSA Public Key Encryption. InCommunication Systems and Network Technologies (CSNT), 2011 International Conference on (pp. 108-111). IEEE.