Detailed Study on Modified RSA Algorithm

Gaurav Patel
L J Institute of Engineering College
Ahmedabad, India

Kunal Panchal
L J Institute of Engineering College
Ahmedabad, India

***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. RSA is highly secure algorithm but have high computation time, so many researchers applied various techniques to enhance the speed of an RSA algorithm by applying various logic. This paper does the detailed study about various techniques and represents the summarized results.**

***Keywords*—RSA, Diffie-Hellman, Cryptography, Cryptosyste, Private-key, Public-key**

I. INTRODUCTION (*Heading 1*)

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 algorithm involves three different phases [2]:

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.

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.

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.

II. RELATED WORK.

A. Additional Prime Number

In this approach the author 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. In this approach Instead of using two primes numbers to generate a public key and private key, they use three primes numbers with reduced size, generates the variable n Large and the process of analysis of the factors is more difficult than the original algorithm. The key strength of the RSA depends on the two prime numbers p and q. The process of factorizing of n will lead to gain the values of p and q. It is much easier to find two numbers from factoring n than finding the value of three numbers from n. in this approach it is very difficult for the attacker to find the three values from factoring n. [3].

B. Modified RSA Approach

The author introduces an 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 intruder to guess the factors of *n* so the encrypted message will be safe from the attacker. Thus this approach provides a more secure path for communication through public key cryptography. In this approach the public key exponent d can be found out by knowing the two prime numbers p and q and which can be known only through n, but as n is not transmitted in public key thus it is very difficult to know the value of d , hence the encrypted message cannot be read easily. It overcomes the limitation of RSA algorithm. [4]

C. Dual RSA

In this methodology of associate RSA whose key generation algorithms output two distinct RSA key pairs that having an equivalent public and personal exponents. This family of variants is understood as twin RSA and it is used for two instances of RSA with the advantage of reducing the info storage necessities of the keys. Two applications for twin RSA, blind digital signatures and authentication square measure projected. The primary application we tend to contemplate is blind signatures. The blind signature permits one user to own a message signed by another user while not revealing any info regarding the message to the signer. There square measure several doable applications for blind signatures like e-cash, untraceable email correspondence, electronic election systems, time-stamping, and anonymous access management. We tend to conjointly give the protection analysis of twin RSA. As compared to traditional RSA, the protection boundary ought to be raised when we are using Dual RSA to the types of Small-d, Small-e, and Rebalanced-RSA. [5].

D. K-Rsa Method

In this method the author constructed a k-RSA algorithm in which the ideas of RSA algorithm and kth power residue theory are combined. This algorithm inherits the advantage of RSA. In this approach we first perform normal steps of

RSA algorithm. We compute the value of phi (*N*). After the factor of phi (*N*) will be determined by the user. In new algorithm, instead of getting *d* by *e.d* =1mod phi (*N*), we have *e.d* =1 mod *k*. because of this values the decryption key exponent values is decrease. If the values of the decryption exponent decrease the time taken for decryption process will decrease and also provides high security. This approach improved security and also achieve a balance between speed and space. 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. Normal RSA is weak and presented a new k-RSA algorithm which is achievable theoretically. It satisfies the requirements of public key cryptography and has faster encryption and decryption speed as compared with RSA. [6]

E. Hybrid Encryption Using Rsa and Diffie-Hellman

Shilpi Gupta and Jaya introduce new concept using two most important algorithm RSA and Diffie-Hellman. RSA and Diffie Hellman both algorithm are combined and proposed new algorithm. The RSA algorithm is be used for public key encryption and digital signature. In this approach the RSA algorithm is used for generation of key. Using RSA we can get public and private key for encryption and decryption process. Diffie Hallman algorithm is used as key exchange method that allows two parties that have no prior knowledge to each other to jointly share a secret key. In this approach the RSA keys were taken as input for Diffie Hellman. The keys are generated using public and private key of RSA algorithm. The Diffie Hallman is used for generating more secure cipher text. For encryption XOR operation is performed between plaintext and key generated by Diffie Hellman algorithm. For decryption process XOR operation is performed between cipher text and key. It will be easy for user to send and receive messages and

F. Hybrid Encryption Using RSA and DES

Gaurav Shrivastava proposes RSA Encryption using DES. The Data Encryption Standard (DES) is the most common Secret Key Cryptography scheme for cryptography. DES so far has been stronger than other cryptosystems in the security. Thus a new scheme to strengthen the DES is needed to protect the cryptosystem. The DES have the same algorithm for encryption and decryption. DES enciphers a block 64 bit of data with 56 bit of key. In approach they will use DES Three Times with RSA Algorithm. The triple DES method provides high security to information/data. After triple encryption the cipher text is encrypted using RSA algorithm. So combing RSA and DES algorithm we can increase the security level. One disadvantage of this approach is that the size of the file is increased because of new approach. [8]

G. RSA Algorithm with Modified Keys Exchange

Sami A. Nagar and Saad Alshamma proposed new technique aims to speed up the implementation of the RSA algorithm during data transmission between different communication networks and Internet. In this approach the key is generated by the program and this key is stored in database. Each key stored in table have index number. This process is known as offline key generation. In this new approach there are four security levels, each level has its own database and number of sets, the level is selected on the basis of the value of E. [9]

H. New Factoring approach

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 normal RSA algorithm the security is deepens on the factoring of value n. If anyone get the value of n and he can successfully get the other values. In new approach there are four values are initially taken. Using this for values we can generate two values of N: N1 and N2. The value of N1 is determined using four variables and the value of N2 is determined using two prime numbers. Because of four variables it is difficulties to factorize value of N1. During the encryption process the sender uses N1. At the receiver side N2 is used for decryption process. 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. [10]

III. SUMMARIZED RESULT:

Sr.	Approach/Method	Remarks
1	Additional third prime number	Because of additional prime number the factoring complexity of variable n is also increase
2	Modified RSA approach	public key exponent d can be found out only by two prime numbers p and q and which can be known only through n, but as n is not transmitted in public key, thus it provides security to message
3	Dual RSA approach	Less than 10% of total time for generating a key pair is assigned to perform the main processor tasks and the other 90% is for crypto-coprocessor tasks.
4	Idea of kth power residue theory	This algorithm not only inherits the advantage of RSA, whose security depends on the difficulties of factoring large integers and finding discrete logarithms, but also has high flexibility of parameters.
5	Hybrid Encryption Using Rsa And Diffie-Hellman	The RSA algorithm is used for public key encryption and digital signature. Diffie Hallman algorithm is used as key exchange method that allows two parties that have no prior knowledge to each other can share a secret key.
6	Hybrid Encryption Using RSA And DES	In approach they will use Triple DES algorithm with RSA Algorithm.
7	RSA Algorithm with Modified Keys Exchange	In this approach keys are stored in database. So the generations of Key is Offline. This approach is faster than normal algorithm.
8	Factoring approach	In this approach the N1 and N2 is generated using four variables. For encryption N1 is used and for decryption N2 is used. Because of this approach it is very difficult to factor N1 and N2.

REFERENCES

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

[2] http://en.wikipedia.org/wiki/RSA_(cryptosystem)

[3] Al-Hamami, A. H., & Aldariseh, I. A. Enhanced Method for RSA Cryptosystem Algorithm. In Advanced Computer Science Applications and Technologies (ACSAT), IEEE 2012 [International Conference, pp. 402-408].

[4] Chhabra, A., & Mathur, S. (2011, October). Modified RSA Algorithm: A Secure Approach. In Computational Intelligence and Communication Networks (CICN),IEEE 2011 [International Conference, pp. 545-548].

[5] 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.

[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] TT II, C. C. H. H. A. A. R. R., and CCLL EE. "Analysis Improved Cryptosystem Using DES with RSA.

[9] Nagar, Sami A., 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, 2012.

[10] 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).

[11] Ivy, B. Persis Urbana, and Purshotam Mandiwa Mukesh Kumar. "A modified RSA cryptosystem based on 'n' prime numbers."

[12] Detail Study : http://en.wikipedia.org/wiki/.NET_Framework.

[13] Detail Study : http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[14] Detail Study : https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture12.pdf