Overview of Improvements and Modifications in RSA Algorithm

[1]Kalpesh S. Prajapati & [2]Prof. B. V. Buddhdev
[1]ME student, Department of Information Technology, SSEC, Bhavnagar, Gujarat, India
[2]Professor, Department of Information Technology, SSEC, Bhavnagar, Gujarat, India

Abstract- **In the today's communication development push the people to transmit their information for so many purposes using the interconnected networks. They are using the internet for credit card payments, tax returns, banking etc. In such a case network security is the very important concept because they have to protect their information from unauthorized users. Cryptography is the way of hiding information during transmission over a channel. There are lots of cryptographic algorithms available to protect our data from intruders. RSA cryptosystem is widely used in the popular Public Key Infrastructure (PKI) implementations and also one of effective public-key cryptographic algorithm. Many research papers submitted on this cryptographic algorithm. Each paper has different perspective. This paper mainly focuses on improvements and modification done in RSA algorithm**

***Index Terms*— Cryptography, Cryptosystem, Encryption, Decryption, private-key, public-key, RSA.**

I. Introduction

Cryptography is derived from Greek word. It has 2 parts: 'crypto' means "hidden, secret" and 'graphy' means "writing". It is a study of techniques for secure communication in the presence of third parties to maintain information securities such as data integrity, confidentiality, authentication, and non-repudiation. A number of algorithms have been proposed for public-key cryptography. Some of these, though initially promising, turned out to be breakable [1]. The RSA cryptosystem was first developed more than 25 years ago by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977 at MIT and first published in 1978. The Rivest-Shamir-Adleman (RSA) cryptosystem most widely accepted and implemented general-purpose approach to public-key cryptography. The RSA scheme is a block cipher in which the plaintext and cipher text are integers between 0 and n - 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024}. It has been widely used for many years on the internet for security and authentication in many applications including credit card payments, email and remote login sessions [1].

RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to log2(n) + 1; in practice, the block size is I bits, where 2i <n < 2i+1. Encryption and decryption are of the following form, for some plaintext block M and cipher text block C.
Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = {e, n} and a private key of PR = {d, n}.
For this algorithm to be satisfactory for public-key encryption, the following requirements mandatory to be met.
1. It is possible to find values of e, d, n such that Med mod n = M for all M < n.
2. It is relatively easy to calculate M^e mod n and Cd mod n for all values of M < n.
3. It is infeasible to determine d given e and n.

II.RSA Cryptosystem

RSA algorithm involves three steps:

(a) Key Generation:

RSA involves public key and private key. Public key is used for encryption and private key is used for decryption of message.
The key generation takes place in the following way:

STEP 1:
Take any two large value prime numbers x and y.

STEP 2:
Compute z by using the given formula
z = x * y

STEP 3:
Compute Phi (z):
Phi (z) = (x-1) * (y-1)
Here, Phi (z) is Euler's totient.

STEP 4:
Choose the public key exponent e such that
1 < e < Phi (z) and, e and Phi (z) are co-prime
Which means that GCD (e, Phi (z)) = 1

STEP 5:
Determine private key exponent d through the given formula: d *e= 1*mod (Phi (z))
This means that d is the multiplicative inverse of
e *mod (Phi (z)).
Thus the public key consists of public key exponent e and n. And private key consists of n and private key exponent d.
Public Key: (z, e)
Private Key: (z, d)

(b). Encryption:
For encrypting a message, first the algorithm convert the given message into an integer number by using a suitable padding scheme.
Then following formula is used to generate encrypted message C: C = M ^ e mod (z)

(c). Decryption:
Following formula is used to decrypt the encrypted message:
M = c ^ d mod (z)

III. Improvements and modification in RSA Algorithm

To overcome the disadvantages of RSA algorithm, some improvements and modification needed to reduce the time, memory, complexity and bandwidth. In order to achieve this there are so many algorithms have been developed. They are as follows.

1. Use of Crypto-Coprocessor and a True Random Number Generator
Bahadori M. implemented novel approach for secure and high speed implementation of RSA algorithm, by implementing on a typical Smartcard equipped with a crypto-coprocessor and a true random number generator. An efficient method for generating the large random prime numbers significantly reduces the total time required for generating a key pair. Algorithm achieved up to 50% reduction in total generation time compared to the latest reported methods. [4]

2. RSA with DES
Gaurav Shrivastava proposes a new approach to enhance the security of cryptosystem. The Data Encryption Standard (DES) is block cipher & the most general 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. [15]

3. Hybrid Algorithm with DSA, RSA and MD5
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. [14]
4. Decryption method base on CRT and strong prime of RSA criterion
Ren-Junn Hwang and Yi-Shiung Yeh proposed an efficient method to employ RSA decryption algorithm. RSA algorithm has to achieve modular exponentiation with large exponent and modulus for better security. The RSA cryptosystem takes great computational cost. In many RSA applications, user uses a small public key to speed up the encryption operation. However, the decryption operation has to take more computational cost to perform modular exponentiation by this case. Ren-Junn proposed an efficient decryption method not only based on Chinese Remainder Theorem (CRT) but also the strong prime of RSA criterion. The proposed decryption method was taking 10% computational costs of the conventional decryption method. It also reduces around 66% computational costs than that of decryption methods based on CRT only. In a word, the speed of proposed method is almost 2.9 times faster than the decryption method based on CRT only. The proposed method enhances the performance of the RSA decryption operation [6].

5. Dual RSA
Dual RSA have been introduced by sun et al. In dual RSA two instances of RSA will share the same public and private key exponents. So it will reduce the memory requirements required for storing both keys because both key exponents are same. Twin RSA is also used to reduce storage requirements. Here there are two different RSA instances such as T1=r1s1, T2=r2s2. As usual we have public key (e) and private key (d). These keys should satisfy the following equations such that ed≡1 mod Ø (T1) and also ed≡1 mod Ø (T2) [9].

6. RSA algorithm with modified keys exchange
Sami A. Nagar and Saad Alshamma speedup the RSA algorithm through a new generation keys method called *RSA-Key Generations Offline* to generate and save all keys values in tables within database. They proposed four security levels, in which

each level has its own database and numbers of sets, these levels identified according to the *e* values and key length, before using the RSA algorithm between gateways must get a *Ready Acknowledgment* from RSA Handshake Database protocol, this protocol is responsible for creation or update the identical gateways database, level selections and establishment the algorithm between gateways. Nagar and Alshamma proposed a new method of keys exchange to increase the difficulty for any one knows the exchanged values between gateways, and then try to get the n, e and d values, This approach was known as Concept of Keys Exchange, where algo exchanges the indexes Nid, Eid, Did instead of n, e, d values.

7. Concept of Kth Residue

Wang Rui, Chen Ju, Duan Guangwen developed k-RSA algorithm in which the idea of kth power residue theory and RSA algorithm were combined. 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 had high flexibility of parameters. It is designed for improved security and had agreed balance between speed and space. At the same time, it can realize functions like hierarchical system management, secret sharing and so on. The result shows that, in k-RSA algorithm d is smaller than e. And that's why new algorithm can largely reduce the computation time of decryption. [11].

8 .Rebalanced RSA

Rebalanced RSA introduced by Wiener in 1990 used to give the good improvement in RSA decryption and also encryption. Normally we have to choose the small public key exponent [8]. But we should not choose the small private key exponent because it is unsafe. So here's wiener is mainly discuss the

weak spot of the use of the private exponent in algorithm .In this algorithm public exponent e is very smaller than the modulus, so automatically it will reduce the encryption costs when we are going to maintain low decryption costs. If we choose a private exponent L so that both L_r and L_s are small. So Rebalanced RSA is mainly used to balance encryption time and decryption time. It is also used to balance the cost and also the memory. Rebalanced RSA reduces the overall cost of encryption and decryption process and rebalance the difficulty of encryption and decryption. It is well suitable for many practical applications. It is just like the same calculation that is done in RSA-CRT for encryption and decryption. The only difference is that we modify this algorithm by choosing the public exponent much smaller than Z can be used [10].

9. Using Short Range Natural Number (SRNN) Algorithm

The Short Range Natural Number (SRNN) algorithm [13] is similar to RSA algorithm with some modification, with enhanced security of the cryptosystem. In this algorithm we have an extremely large number that has two prime factors (similar to RSA). Moreover Algorithm uses two natural numbers in pair of keys (public, private) .These natural numbers increase the security of the cryptosystem. So its name is "Modified RSA Public Key Cryptosystem using Short Range Natural Number Algorithm" that used short range in both algorithms they found that by increasing modulus length n security increase, speed decrease and when chunk size m increases both security and speed increases. From key generation point of view SRNN algorithm is bit of slower than RSA algorithm. From encryption point of view both algorithms are working almost same .In case of SRNN algorithm only one multiplication operation is additional for each chunk calculation. So when chunk size increases, both algorithms are giving almost same time. From decryption point of view SRNN algorithm is much slower than RSA algorithm. Overall performance of SRNN algorithm is better in security but slower in speed. When modulus length is increases speed of SRNN algorithm is decreases with respect to RSA algorithm. Difference of SRNN and RSA with modulus length 1024 bits are approximately 5080 milliseconds (SRNN 1024 bits > RSA 1024 bits) whereas difference of RSA 2048 bits and SRNN 1024 bits are 5338 milliseconds (RSA 2048 bits > SRNN 1024 bits). Hence SRNN with modulus length 1024 bits are is good balance between speed and security.

IV. Conclusion

In this paper, we surveyed different methods modified by various researchers and scholars for faster implementation and security enhancement of 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 13: 978-0-13-609704-4, Pearson Education, Fifth Edition.

[2]. W. Stallings, "Network security Essentials: Applications and Standards" ISBN 13: 978-0-13-610805-4 Pearson Education India, Fourth Edition.

[3]. Atul Kahate "Cryptography and Network Security" 3rd edition.

[4] M. Bahadori, M. R. Mali, O. Sarbishei, M. Atarodi and M. Sharifkhani "A novel approach for secure and fast generation of RSA public and private keys on Smartcard" NEWCAS Conference (NEWCAS), 2010 8th IEEE International, 2010, pp. 265-268.

[5]. R. Rivest, A. Shamir, and L. Adleman, "A Method for obtaining Digital Signatures and Public-Key Cryptosystems, "ACM Trans. On Communications, vol. 21, pp. 120-126, 1978. (Founder of RSA in 1977)

[6]. H. Ren-Junn, S. Feng-Fu, Y. Yi-Shiung and C. Chia-Yao "An efficient decryption method for RSA cryptosystem" (AINA 2005). 19th International Conference on, 2005, pp. 585-590 vol.1.

[7]. Hongwei Si, Youlin Cai, Zhimei Cheng, "An improved RSA Algorithm based on Complex numeric operation function".

[8]. Wiener M., "Cryptanalysis of short RSA secret exponents", IEEE Trans. Inform. Theory 36(1990), 553-558.

[9]. H.M. Sun, M.E. Wu, W.C. Ting, and M.J. Hinck, 'Dual RSA and its Security Analysis', IEEE Trans. On Information Theory, vol.53, no.8, pp. 2922-2933, August 2007.

[10]. H/-M. Sun, M.J. Hinek, and M.-E. Wu, "On the design of Rebalanced-RSA, revised version of Centre for Applied Cryptographic Research", Technical Report CACR 2005-35, 2005

[11]. Wang Rui; Chen Ju; Duan Guangwen, "A k-RSA algorithm," ICCSN, 2011 IEEE 3rd International Conference on, vol., no., pp.21, 24, 27-29 May 2011

[12]. Nagar, S.A.; Alshamma, S., "High speed implementation of RSA algorithm with modified keys exchange," Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on , vol., no., pp.639,642, 21-24 March 2012

[13]. Sharma Sonal, Jitendra Singh Yadav, and Prashant Sharma. "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm." International Journal 2.8 (2012).

[14]. Kaur, Khushdeep, and Er Seema. "Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices" IJERA, 2.5 (2012): 914-917

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