Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Critical Analysis of RSA Public Key Cryptosystem

Ritu Tripathi
Department of CEA,
National Institute of Technical Teachers' Training and Research,
Bhopal, India

Sanjay Agrawal
Department of CEA,
National Institute of Technical Teachers' Training and Research,
Bhopal, India

Abstract— ***In Public key cryptosystem two different a pair of keys are used, one for encryption through private key and other for decryption through public key .The advantage of this cryptosystem is that no other one can decrypt the text and message without this pair of keys. This paper surveys on public key generation RSA algorithm and various Improved RSA algorithm by applying various modifications in existing algorithm. RSA is highly secure algorithm but have high computation time and slow speed, so many researchers impractical various techniques to increase the speed of an RSA algorithm by applying various modification. This paper does the detailed study about various techniques and represents the summarized results through used different open source.***

Keywords— ***Public key cryptosystem; RSA scheme.***

I. INTRODUCTION

A. *Cryptography:*

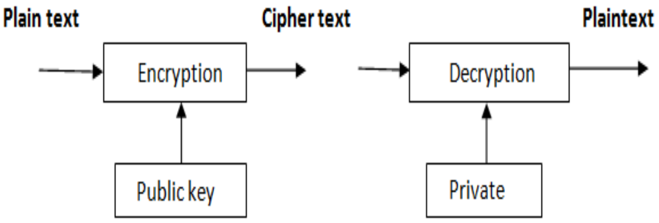
We have seen over in last year's an increase in demand for data communication and internet services so protection of data from the third party. Therefore, secure techniques for communication in presence of hacker such as cryptography are used. Cryptography is a needful tool for protecting information or writing in network. This methods involve two basic activities first one is hiding information from unauthorized parties and second one is making information meaningless(unintelligible) to individuals other than intended recipient. There are two types of encryption key symmetric (secret key) and asymmetric (public key).

B. *Symmetric and Asymmetric Algorithms:*

Symmetric algorithm uses the same key for encryption and decryption. This is called secret key. Asymmetric algorithms use a different key .one key(public) is used for encryption and other(private key) is used for decryption. This is called public key.

C. *Public key cryptography:*

Public key cryptography is one of the most important technique which was invented by Whitfield Diffie , Martin Hellman and Ralph Markel in 1976.They proposed that to provide more secured data communication instead of single secret key , pair of key can be used an encryption key and decryption key and the decryption key cannot be derived from the encryption key. An encryption key called the public key, is disclosed and decryption key called the private key, is kept private.



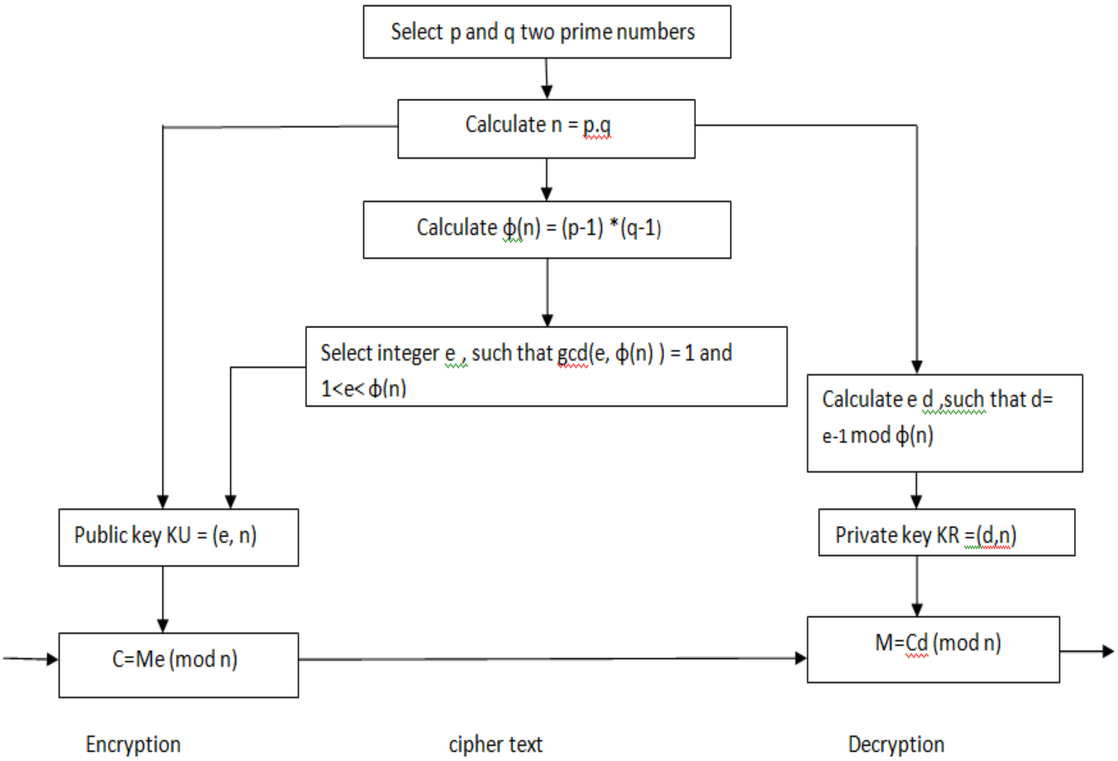
1.1 Public key cryptosystem

The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure.

II. RSA CRYPTOSYSTEM

RSA is the most important public key cryptosystem. This algorithm was invented by Ronald Rivest, Adi Shamir and Leonard Adelman at MIT in 1977. RSA authentication is known to be the most widely adopted encryption method. There are two keys used in RSA algorithm (public key and private key).one key (public key) is used for encryption and other key (private) is used for decryption.

The security of RSA depends on the difficulty of factoring large integers. Difficulty of factoring n to find the original primes p and q defines the strength of RSA. So larger the value of primes. Again, typical values for these primes are 512 to 4096 bits. We can easily understand through the flow chart of RSA algorithm.


Select p and q two prime numbers
Calculate n = p.q
Calculate ϕ(n) = (p-1) *(q-1)
Select integer e , such that gcd(e, ϕ(n)) = 1 and 1<e< ϕ(n)
Calculate e d ,such that d= e-1 mod ϕ(n)
Public key KU = (e, n)
Private key KR =(d,n)
C=Me (mod n)
M=Cd (mod n)
Encryption
cipher text
Decryption

A. ***Security of RSA***

The security of RSA algorithm depends on the ability of the hacker to factorize numbers. New, faster and better methods for factoring numbers are constantly being devised. Obviously the longer a number is the harder is to factor, and so the better the security of RSA. As theory and computers improve, large and large keys will have to be used. The advantage in using extremely long keys is the computational overhead involved in encryption/decryption. This will only become a problem if a new factoring technique emerges that requires keys of such lengths to be used that necessary key length increases much faster than the increasing average speed of computers utilizing the RSA algorithm. RSA's future security relies solely on advances in factoring techniques.

B. ***RSA methodology:***

RSA involves distribution of public key and private key to sender and receiver to encrypt and decrypt the message respectively. RSA is a three steps process that involves key generation, Encryption and Decryption.

1) Key generation:

Step 1: Choose two distinct large random prime numbers p and q.

Step 2: Compute n=p*q. the number n is used as the modulus for both public and private keys.

Step 3: Computer the Euler's function: ϕ (n) = (p −1) (q −1).

Step 4: Choose an integer e, 1< e< ϕ (n); such that GCD (e, ϕ (n)) = 1,e and ϕ (n) are co prime . e is used as a public key exponent.

Step 5: Compute d, 1< d< ϕ(n) such that ed = 1(mod ϕ (n)) , d is used as a private key exponent.

Public key consists of public key exponent e and n and Private Key consists of private key exponent d and n.
Public key: (e, n) and private key: (d, n).

2) Encryption:

The Sender sends the original message as a plaintext (M) and after encryption message convert to the cipher text (C).
Plaintext : M <m
Cipher text : C =M^e mod (n).

3) Decryption:

The receiver receives the message as a cipher text(C) and after decryption cipher text message convert to the original message (M).
Cipher text: C
Plaintext : M = C^d mod (n).

III. RELATED WORK

A **.** *Using 'N' Prime Number:*

B.persis Urbana Ivy, Purshotam Mandiwa , Mukesh Kumar Proposed modified RSA cryptosystem to handle 'n' prime numbers and provides maximum security . In this implemented method we used 'n' prime number which is not easily breakable and this numbers are not easily decompose. This method provides more efficiency and reliability over the networks.

B. *Using Short Range Natural Number Algorithm*:

Sonal Sharma, Jitendra Singh Yadav , Prashant Sharma In this paper proposed short range natural number algorithm .This algorithm is similar to RSA algorithm with some modification. This modification increases the security of the cryptosystem. In this algorithm we have an extremely large number that has two prime factors (similar to RSA). In addition of this we have used two natural numbers in pair of keys (public, private).These natural numbers increase the security of cryptosystem .so its name is "modified RSA public key cryptosystem using short range natural number algorithm". The comparison between RSA and SRNN both algorithm 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 then RSA algorithm. From encryption point of view both algorithm are working same. In case of SRNN algorithm only one multiplication operation is additional for each chunk calculation. So when chunk size increases we found both algorithms are giving almost same time. Decryption point of view SRNN algorithm is much slower then RSA algorithm. Overall performance we found that 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 is approximately 5080 milliseconds whereas difference of RSA 2048 bits and SRNN 1024 bits are milliseconds. Hence SRNN with modulus length 1024 bits are is good balance speed and security.

C**.** *Using Hybrid Cryptography Algorithm:*

Ravishanker Dhakar , Amit Kumar Gupta, Prasant Sharma In this paper presents a hybrid cryptography algorithm which is based on additive homomorphic properties called modified RSA encryption algorithm (MREA). MREA is secure as compared to RSA as it is based on factoring problem as well as decisional composite residuosity assumption which is the intractability hypothesis. This method used additive homomorphic properties means that given only the public key and the encryption of m1 and m2 , one can compute the encryption of m1+m2.

D. *Using K^{th} Power:*

Wang Rui , Chen Ju , Duan Guangwen In this paper we construct a k-RSA algorithm in which the idea of kth power residue theory and RSA algorithm are combined This algorithm not only inherits the advantageof RSA, whose security depends on the difficulties of factoring large integers and finding discrete logarithms, but also has high flexibility of parameters. It is designed for improved security and to achieve a balance between speed and space. At the same time, it can realize following functions: hierarchical system management, secret sharing and so on. The result shows that, in the case of e equality in K-RSA algorithm is similar. And that's why new algorithm can largely reduce the computation time of decryption.

E. *Using Two N Values*:

Dhananjay Pugila, Harsh Chitrala, Salpesh Lunawat, P.M.Durai Raj Vincent In this paper, we describe a new algorithm which is similar to RSA algorithm with some modification. In this algorithm we have used four variables among them two are prime and other two are random numbers. There are two n values n1 and n2. n1 is extremely.

large number which is product of two prime and two random numbers which makes it difficult for hacker to factorize value and n2 is the product of prime numbers. n1 is used during encryption and n2 during decryption. Even if the hacker manages to factorize n1, it will be hard to determine the prime numbers from factors, so that he/she can calculate n2 and decrypt the message. This modification increases the security of the RSA cryptosystem. The result that this approach is more secure than RSA algorithm and advantage of this algorithm is that, the time taken for brute-force attack is more compared to RSA algorithm. Even if the hacker manages to factorize n1, it will be hard to determine prime numbers from factors, so that he/she can calculate n2 and decrypt the message.

F. *Using Subset Sum Cryptosystem*:

Sonal Sharma, Prashant Sharma,Ravi Shankar Dhakar In this paper presents a hybrid cryptography algorithm which is based on the factoring problem as well as Subset-Sum problem called a Modified Subset-Sum over RSA public key cryptosystem (MSSRPKC). The Subset-Sum cryptosystem (Knapsack Cryptosystem) is also an asymmetric cryptographic technique. The Merkle-Hellman system is based on the subset sum problem (a special case of the knapsack problem): given a list of numbers and a third number, which is the sum of a subset of these numbers, determine the subset. In general, this problem is known to be NP-complete. However, if the set of numbers (called the knapsack) is super increasing , that is, each element of the set is greater than the sum of all the numbers before it, the problem is 'easy' and solvable in polynomial time with a simple greedy algorithm. Result shows that both algorithm RSA which is based on single modulus, is broken in time x and Subset sum based algorithms is broken in time y then the time required to break MSSRPKC algorithm is x*y. So the security of MSSRPKC algorithm is increased as compare to RSA algorithm.

SUMMARIZED RESULTS

s. no	Approach/method used	Remarks	Scope of improvements
A	Using 'N' prime number	• This technique we used 'n' prime number which is not easily breakable. 'n' prime numbers are not easily decompose. • Prime number used in a modified RSA cryptosystem to provide security over the networks.	To develop the RSA algorithm for 'n' prime numbers and also used four prime numbers
B	Using Short Range Natural Number 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 number increase the security.	
C	Using Hybrid Cryptography Algorithm	• It is based on the factoring problem as well as decisional composite residuosity assumptions which is the intractability hypothesis. • Additive homomorphic cryptosystem means that, given only the public-key and the encryption of $m1$ and $m2$, one can compute the encryption of $m1 + m2$. • RSA is based on single modulus, is broken in time x and additive homomorphic based on dual modulus, is broken in time y then the time required to break MREA algorithm is x*y. So the security of MREA algorithm is increased	
D	Using Kth Power	• 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 flexibility of parameters.	
E	Using two n values	• This method used two n values n1 and n2. We have used four variables to determine the value of n1. This makes it difficult to factorize n1 value. n1 is used during encryption and n2 is used during decryption and this helps in increasing the security of RSA algorithm. • This algorithm is that, the time taken for brute-force attack is more compared to RSA algorithm.	
F	Using subset sum cryptosystem	• We used subset sum cryptography. The subset sum problem given a list of numbers and a third number, which is the sum of a subset of these numbers, determine the subset. In general, this problem is known to be NP-complete.	

IV. CONCLUSION

In this paper, Public-key cryptography has evolved from early models to more sophisticated systems that have provided the privacy and data security that we need in the modern world. we critical analysis of different types enhanced and modified methods proposed by various researchers and scholars for fast Implementation RSA algorithm. In which we endeavored to get the quality that make easier the cryptography to have a good use prime numbers. They used various techniques and methodology such as 'N' prime number, k residue prime, Short Range Natural Number Algorithm, subset sum cryptosystem, hybrid cryptography algorithm, two n values. It's achieved the requirements of public key cryptography and has faster encryption/decryption speed (high) compared with exiting algorithm .To improve the security, modified public key cryptosystem is developed and these approach is more secure than exiting cryptosystems.

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers for their valuable comments and suggestions on the part of security analysis, which certainly led to improvements of these correspondences.

REFERENCES

[1] William stallings “cryptography and network security” ISBN 81-7758-011-6 Pearson Education,Third Edition.

[2] B.Persis Urbana Ivy , Purshotam Mandiwa. Mukesh Kumar “A modified RSA cryptosystem based on ‘n’ prime numbers” International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume1 Issue 2 Nov 2012.

[3] Sonal Sharma, jitendra singh yadav and prasant Sharma “modified RSA public key cryptosystem using short range natural number algorithm” international journal 2012

[4] Ravishanker Dhakar , Amit Kumar Gupta, Prasant Sharma “Modified RSA Encryption Algorithm (MREA)” 2012 Second International Conference on Advanced Computing & Communication Technologies

[5] Wang Rui , Chen Ju , Duan Guangwen “A k-RSA Algorithm” communication software and networks(ICCSN), 2011.

[6] Dhananjay Pugila, Harsh Chitrala, Salpesh Lunawat , P.M.Durai Raj Vincent “An Efficeient Encrpytion Algorithm Based On Public Key cryptography” International Journal of Engineering and Technology (IJET) , Vol 5 No 3 Jun-Jul 2013.

[7] Sonal Sharma, Prashant Sharma, Ravi Shankar Dhakar “RSA Algorithm Using Modified Subset Sum Cryptosystem” International Conference on Computer & Communication Technology (ICCCT)-2011.

[8] Rohit Minni, Kaushal Sultania, Saurabh Mishra, Prof Durai Raj Vincent PM “An Algorithm to Enhance Security in RSA” International Conference on Communication and Computer network Technology 4th ICCCNT 2013.

[9] V.Saravanakumar “ERSA: Secure and Enhanced RSA” International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4, Jul-Aug 2013.

[10] Sushanta Kumar Sahu ,Manoranjan Pradhan “FPGA Implementation of RSA Encryption System” International Journal of Computer Applications, Volume 19– No.9, April 2011.

[11] Nitin R. Mise, H. C. Srinivasaiah “ A Mathematical Attack Based Algorithm to Challenge the Security of RSA Cryptosystem” International Journal of Advancements in Research & Technology, Volume 2, Issue 6, June-2013.