www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-1, Issue-2, June- 2013
Research Paper

Int. J. Sci. Res. in
Network Security
and Communication
ISSN: 2321-3256

Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and ‘n’prime Number

V. Kapoor

*Department of Information Technology
Institute of Engineering and Technology, DAVV, Indore, India

vkapoor13@yahoo.com

Received: 26 April 2013 Revised: 12 May 2013 Accepted: 06 June 2013 Published: 30 June 2013

Abstract: Now a days, have a great dependence on computer and network and the security of computer related to the whole world and everybody. Cryptography is the art and science of achieving security by encoding message to make them non-readable [1] to secure data or information transmits over the network. In this paper introduced modified RSA approach based on multiple public keys and n prime number.RSA algorithm is mostly used in the popular implementation of public key cryptography. In public key cryptography two different keys are generated in RSA one keys is used in encryption data and other corresponding key used for decryption. No other key decrypt the data. Even if it is efficient algorithm it is vulnerable to other person. With the help of all brute force attacks can obtain private keys. In this research paper new approach we used n prime number and multiple public keys. Which is not easily crack able .In here implementation RSA algorithm .using some mathematical logic integer factorization and discrete logarithm problem.

General Terms - Data security, Encryption, Authentication, Data transmission.

Keywords - Cryptography, RSA algorithm, Triple DES, Asymmetric key Cryptography, ’n’ prime number.

I. Introduction

In the today’s era the internet provides communication between people and facilitates for electronic payment, military communication and many others. This cause a major concern for privacy, identify theft, security etc. cryptography is a standard way of secure the data over the medium.

Cryptography has been developed from the Greek word krypto and graphein which means is hiding information person who study and discover cryptography are called cryptographers and study of cryptography is name by cryptanalysis.

Cryptography is a part of secret information .it is science and art of protecting the information over the medium. It is process of convert readable text to unreadable text. By using the cryptography we can help this fickle information by private document on over computer network.

In a distributed network cryptography become important part of secure communication .there are three type of cryptography algorithm: symmetric key cryptography, Hashing, Asymmetric key cryptography.

An algorithm for cryptography that uses the same keys for both encryption of normal text and decryption for cipher text is called symmetric key cryptography .e.g. Data Encryption standard(DES) and Advance Encryption standard(AES).To solve the key distribution problem Maryam Ahmed [11]developed the concept of public key cryptography in 1976.

Rivest, Adi Shamir and Leonard Aldeman are discover RSA in 1977.it generates two key: public key for encryption and private key to decryption message [3].RSA algorithm consist of three phase: first phase key generation, second phase is encryption and third phase is decryption.

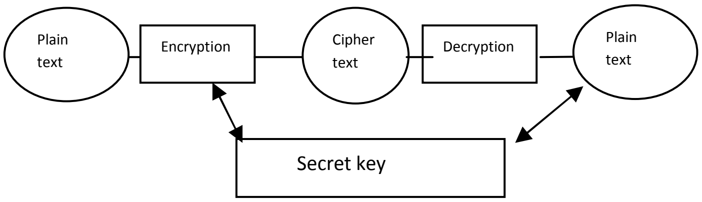
As a public key is used for encryption and is well known to everyone and with the help of public key, attacker can use brute force method to find private key which is used to decrypt message [4].

The proposed algorithm is similar to RSA with few modification .Proposed algorithm is also known by public key cryptography .In this algorithm we have taken extremely large number that has four prime factor (similar to RSA) in addition of this used to two public keys.

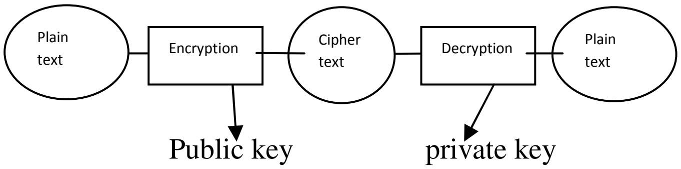
II. Related work

Cryptography is a process which is associated with encloses plaintext into cipher text (encryption process) then back again plaintext (decryption).In Asymmetric key cryptography using two different keys: public key and private key .private key cannot obtain by public key.

This is one major difference between asymmetric and symmetric key cryptography, and that major difference change whole process. mostly it has implication throughout the security .As compare symmetric key cryptography as faster move easy and better suited for application drawback of symmetric key cryptography is less secure and move open to wider areas of attacks.



Symmetric Key Cryptography



Asymmetric Key Cryptography

III. Literature review

Rivest, Shamir and Aldemam-RSA methodology for confidentially and authentication in this research paper which is used RSA algorithm for secure transmission over the computer and network. It is also increased the efficiency and security.

According to Ravi Shankar: - security of RSA algorithm depends on prime number because it is difficult to crack the large prime number. It is provide the security and performance. In this paper a modified RSA algorithm is provide security against brute force attack.

Hu-Zhou: in this research paper which is used large prime number RSA cryptography for security [3].the prime number is not easily factorized.

IV. Problem definition

The positive large number is easily factorized or break and less prime number are easily decomposed which will not provided more security over the network, that's why we used two public key and n prime number to provide more security over the network and it is also not easily break and data sharing between different nodes are vulnerable.

V. Solution methodology

In this research paper we developed an algorithm it is based on modification RSA algorithm based on two public key and n prime number. This algorithm provides high security over the network and secure data transfer on the transmission medium [12].

Computational steps for Mathematical foundation and key generation in RSA of algorithm

A:-The RSA digital signature has appropriate mathematical foundation, which as follow [5]

Theorem 1: Any positive Integer a can be denoted by ai where

$A_i=p_1\ p_2,\ p_3$------------------------------p_n, ɏ p_n , **ai>0**

Theorem 2 :(Euclid theorem): the greatest common divisor g of the positive integer a and b can be represented as a liner sum of original two number a and b .in other world, it is always possible to integer s and t such that –

g =s*a +t*b [6]

Theorem 3 :(Fermat little theorem): it state that if p is a large prime number, then for any positive integer a, then a^p=a mod (p) or a^{p-1}=1 (mod p)

Theorem 4: if p and q are prime number and p not equal to q then

ϕ (p q) = ϕ (p)*ϕ (q) = (p-1) (q-1)

B: RSA key generation algorithm-

1. Select two different large random prime number p and q.
2. Calculate n=p*q and ϕ (n) = (p-1)*(q-1) [theorem 4]

Where ϕ is an Euler's function

3. Choose an integer e, such that 1<e< ϕ (n) and gcd (e, ϕ (n)) =1 [theorem 2] where e, ϕ (n) are co-prime.
4. Compute d;

d is multiplication inverse of e mod (ϕ (n))

e *d mod ϕ (n) =1

5. The public key is (e, n) and private key is (d, n).

Encryption:-

Sender A know the following

1-Recive the receiver B's public key.
2-The plaintext message as a positive Integer m.
3-calculate the cipher text C=m^e mod

4-calculated C sends to B

Decryption:-

Receiver B does the following
1-Using private key to compute $m=c^d$ mod n
2-Get original plain text m

Proposed RSA algorithm

RSA is 1024 bit block cipher in which the plain text and cipher text integer value lie between 0 to n-1.

In which we will be used four prime number and get public key and private key [7] and also using two public keys and one private key for encryption and decryption

RSA key generation

1-computational steps for selecting the largest prime number p, q, r and s in RSA cryptography.

-Firstly, we decided upon the size of integer and implementation if RSA of size B Bits.

-To generated the prime integer p, q, r and s;

-Using the high quality random number generator [8].you first generated a random number of size B/2 bits.

-We set the lowest bit of integer generated by the above step: this ensures that the number will be odd [9].

-We also set the two highest bits of the integer: this ensures that the highest bits of null are set.

-Using the Miller–Rabin-theorem, check to see if the resulting integer is prime .if not you can increment by 2 and check again.

2- Calculate $n= p*q*r* s$ and $\phi (n) = (p-1) (q-1) (r-1) (s-1)$ Where ϕ is Euler's function.

3-choose an integer value e, where e lies between 1 to $\phi (n)$ and gcd $(e, \phi (n)) =1$.

Select two number a and b such that $b=a*e$ and using this number two public key {b, e}, {a}[10].

4-finally compute d as multiplication inverse of e mod ($\phi (n)$)

Encryption: Suppose that user A has shared its public key and that user B send the message m to A.

Then B calculate cipher text $C= (m^{b/a})^{d}$ mod n and then send C.

Decryption of the cipher text by A and user A decrypt message $m= c^d$ mod $n= (m^{b/a})^d$ mod $n =m^{b/ad}$ mod n.
Both sender and receiver must known about the values of n,b and a only receiver known the secret value of d In asymmetric key cryptography with public key K.U={b,n},{a} and private key of K.R ={d,n}[10]

Comparison among RSA, Modified RSA using two public key and MRSA using n prime number

Table i shows the general compare among RSA, Modified RSA and MRSA using n prime number .in this algorithm we found that by increasing module length n then increase security and speed decrease.

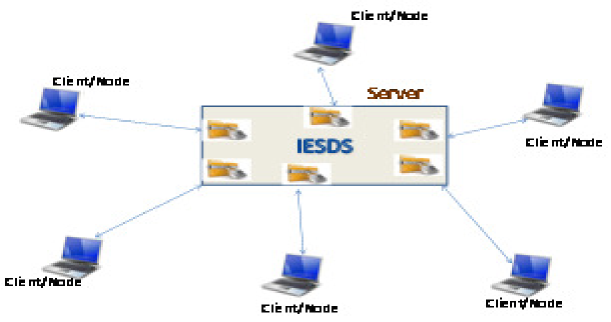
Key generation point of view MRSA, MRSA with n prime number is slower than RSA. In encryption point of view all are working almost same. In case of algorithm only one multiplication operation is additional for each fragment calculation.
For decryption point of view MRSA, RSA is almost same .overall performance vice MRSA with n prime number is better in security but less in speed and throughput.

Comparison among RSA, MRSA and MRSA with n prime number

s.no .	RSA	MRSA	MRSA with n prime number
1.	Use only one public key	Use 2 public key	Use 2 public key
2.	Less communication overhead	Medium communication overhead	High communication overhead
3.	Process speed is fast	Process speed is slow	Process speed is very low
4.	It has less security	It is increasing security	It is provide more security
5.	More permeable to brute force attack	Less permeable to brute force attack	Little permeable to brute force attack
6.	Using encryption and decryption required time is more.	Using encryption and decryption required time is less.	Using encryption and decryption required time is more less.

Table no.i

VI. System Overview



With the recent seizure and spread of the data sharing paradigm in distributed systems such as online social networks or cloud computing, there have been increasing demands and concerns for distributed data security. Improving security and efficiency in data sharing over the transmission medium and network [14].

In IESDS three levels of Authentication are provided with a dedicated architecture.

First Level: It is the User, who is having all the privileges i.e. can add data, can add node, can share to specific node or can sharing to all the workstations members.

Second Level: Here only authentication nodes access server.

Third Level: After second level verification, node access folder created by self then this permission granted by Data Access Control level.

VII. Conclusion and future work

In this research paper an algorithm is proposed for RSA a method for implementing a public key cryptography (RSA) using two public and four prime number and same mathematical equations. Using two public keys and n prime number, which is provide the security over the network so attacker cannot get keys and unable to decrypt the message. The proposed modified RSA approach is used for system that provides more security but less speed compare to RSA algorithm and improving security and efficiency in data sharing over the network. This proposed work would be inspiring for advance research such as secure transmission of file, video file, image file, etc. this may perhaps our future research topic using hybrid data encryption and decryption approach[13].

VIII. REFERENCES

[1]. AAtul Kahate, Cryptography and Network Security, Tata McGraw-Hill Publication Company Limited page no. 32 **2003**.

[2] Xiaowen Kang; Inst. of Electron. Technol., PLA Inf. Eng. Univ., Beijing; Yingjie Yang; Xin Du,” A Disaster-Oriented Strong Secure File System” Innovative Computing Information and Control, **2008**. ICICIC '08. Pages 557.

[3] Xin Zhou, Xiaofei Tang,”Reasearch and Implementation of RSA algorithm for Encryption and Decryption “IEEE 6th International Forum on strategic Technology pp 1118-1121, **2011**.

[4] Rajan.s.jamgekar, Geeta shantanu joshi “File Encryption and Decryption using secure RSA” International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February **2013**.

[5] P.Saveetha & S.Arumugam “Study on Improvement in RSA Algorithm and its Implementation” International Journal of Computer & Communication Technology ISSN (PRINT): 0975 - 7449, Volume-3, Issue-6, 7, 8, **2012**

[6] en.wikipedia.org/wiki/Euclidean algorithm

[7] 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** Page No. 63-66

[8] en.wikipedia.org/wiki/Random_number_generation

[9] Avinash kak, Purdue University Lecture Notes on “Computer and Network Security”June 20, **2003**

[10] Milad Bahadori1, Mohammad Reza Mali, Omid Sarbishei, Mojtaba Atarodi, Mohammad Sharifkhani,”Novel Approach witch is the Secure and Fast Generation of RSA Public and Private Keys on Smart-Card”, 978-1-4244-6805-8/10/$26.00 **2010** IEEE.

[11] Maryam Ahmed, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei, Habeeb “Diffie-Hellman and Its Application in Security Protocols” International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November **2012**

[12] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, “A Content-Driven Access Control System,” Proc. Symp. Identity and Trust on the Internet, pp. 26-35, **2008**.

[13] Rangarajan A. Vasudevan, Sugata Sanyal” Jigsaw-based Secure Data Transfer over Computer Networks” Information Technology: Coding and Computing,. Proceedings. ITCC 2004. International Conference on (Volume:1) **2004.**

[14] Wuling Ren, Zhiqian Miao, College of Computer and Information Engineering, Zhejiang Gongshang University, “A Hybrid Encryption Algorithm Based on DES and RSA” in Bluetooth Communication Second International Conference on Modeling, Simulation and Visualization Methods **2010**.