IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
ISSN : 2348 - 6090
www.IJCAT.org

Implementation of Modified RSA Cryptosystem Based on Offline Storage and Prime Number

[1] Ms. Ritu Patidar, [2] Mrs. Rupali Bhartiya

[1] Shri Vaishnav Institute of Technology & Science, Indore, India
Department of Computer Science Engineering, SVITS, Indore, India

[2] Shri Vaishnav Institute of Technology & Science, Indore, India
Department of Computer Science Engineering, SVITS, Indore, India

Abstract - For secure communication over the network, there are various cryptographic techniques but the most famous public cryptographic technique is RSA cryptography. Cryptography is knowledge of protecting the information for providing encryption techniques. It is the most advantageous solution for the security of information in computer network. For providing confidentiality in the network and improve the speed of RSA algorithm, we developed an implementation of modified RSA algorithm which is based on offline storage and prime number. This paper describes the practical implementation of proposed RSA method in matlab (R2012b) .

Keywords **- RSA, cryptography, indexes, public key, private key, Offline storage, prime number.**

1. Introduction

The earliest form of cryptography was the simple writing of a message, as most of the persons could not read. The word cryptography comes from the greek words krypto which means hidden. If you want to keep the information secret, there are two possible strategies- hide the existence of the information or make the information secure from intruders. The earliest form of cryptography was the simple writing of message, as most of the persons could not read. At present the best known and most widely used public key algorithm is RSA which was the first public key algorithm invented in 1977. It became the international standard of public key cryptography. It uses pair of related keys, one for encryption and other for decrypt. One key which is called private key is kept secret and one is public key is disclosed to everyone in the network. It is the most popular approach refers asymmetric cryptography that can be used both data encryption and digital signature. Modern cryptography is based on mathematical theory which is based on computer science engineering. It is synonymous with encryption. Encryption is the process in which the conversion of message from readable to non readable state.

RSA cryptosystem is one of the famous security algorithm which is composed of three phases- key generation, encryption process and decryption process. Many experts, researchers and developers have to build and enhance the security system, protect the information and prevent the attackers from playing with the important source of information. In proposed method, some concepts of existing RSA method are added to provide higher security and improve speed .This paper enhances the proposed RSA algorithm through practical implementation.

1.1 Secure Communication Using RSA Algorithm

RSA algorithm refers to public key cryptography method. It is an asymmetric technique, based on two different key pair's public and private keys. It is based on mathematical operations and it is feasible for user to generate his or her public and private key pair for encryption and decryption with the help of PSA algorithm. In a secure communication using public key cryptography (RSA algorithm) following procedure are taken-

1) The sender encrypts the message using receiver's public key, this key is known to everyone in the communication network.
2) The encrypted message sends to the receiving end that will decrypt the message with its private key.
3) Only the intended receiver can decrypt the message because only receiver knows the private key.
4) Thus using RSA algorithm we can communicate in a secure way.

1.2 Problem with Existing RSA Cryptosystem

In existing RSA algorithm provides less security over the network. It uses public key cryptography for encryption and decryption. Its computation takes time to compute the

mathematical operation of RSA algorithm. RSA provides communication secure but still there are many problems with RSA cryptography which are states below:-

1. Its computation takes time to compute the mathematical operation of RSA algorithm.
2. Public key used for encryption should be authenticated.
3. If hacker knows the factors of a large prime number then this break the security of algorithm, because the values of public key and private are known with help of factors.
4. There are various attacks in RSA cryptosystem such as factorization problem, low encryption exponent, common modulus etc. These attacks can break the security of RSA cryptography.

2. Literature Survey

Background: - The background study is provided so as to get familiar with the basic concepts which are based on public key cryptography techniques.

Shilpi Gupta and Jaya Sharma proposed a hybrid encryption algorithm based on RSA algorithm and diffie hellman algorithm[10]. They proposed an algorithm by combining the two most popular algorithm RSA algorithm and diffie hellman algorithm in order to achieve higher security. RSA algorithm can be used for both public key encryption and digital signature. Diffie hellman algorithm is used to exchange the secret key between two parties and is also used for providing more secure cipher text. RSA keys were taken as input to diffie hellman algorithm. A GUI developed using java applet provides options to the input user message and to upload file. Thus it provides the better efficiency in terms of time complexity. A limitation of this paper is that the key size of this algorithm is large which is modified further by many authors.

Ashutosh Kumar Dubey et.al proposes a novel method cloud-user Security Based on RSA and MD5 algorithm for resource attestation and sharing in java environment [13]. A new secure cloud computing environment established by using both RSA and MD5 algorithm. According to them in that method contains two parts. First part is controlled by user which gets permission by the cloud. Second part shows a secure trusted computing for the cloud. If admin want to read and update the data from cloud it take permission from the client environment. In this way it provides a way to hide the data and normal user, thus it protects their data from cloud provider. When the user upload the data in the cloud , the data are encrypted by using RSA encryption algorithm and cloud admin decrypt the data by its private key. If admin wants to update the data it needs secret key provided by a user through message digest tag which is generated by MD5 algorithm. This paper present the two most secure algorithm used for data gathering and data sharing in the cloud computing environment. The limitation of this algorithm is it is helpful for today's requirement.

A novel approach is proposed by Wuling Ren and Zhiqian Miao for RSA key generation. A hybrid encryption algorithm is implemented which is based on DES algorithm and RSA algorithm in Bluetooth communication [11]. DES encryption is used for the transmission of data because of its higher efficiency in block encryption. RSA algorithm is used for the encryption of keys of DES algorithm because of its better management of keys. Thus it provides dual protection in Bluetooth communication network. In Bluetooth network there are vulnerable attacks are happened thus DES and RSA hybrid algorithm are more secure and easier to achieve. It provides secure data transmission between the Bluetooth devices. The limitation of this algorithm is that the Bluetooth technology has not fully considerate security issues in the standardization process. As compared to the fixed Bluetooth network it is more vulnerable to be attacked.

Sonal Sharma et.al proposed a novel approach RSA algorithm Using Modified Subset Sum Cryptosystem. This system is based on subset sum problem (knapsack problem)[12]. In knapsack problem given a list of third number which is the sum of subset of other two numbers, determines the subset. This paper presents a modified subset-sum over RSA public key cryptosystem (MSSRPKC), MSSRPKC is secure against brute force and mathematical attack on RSA as well as Shamir attacks. The limitation of this algorithm is it is based on one way function therefore it cannot be used for authentication. Another disadvantage is it is slow down the execution process as compare to RSA.

Sami A. Nagar and Saad Alshamma proposed a method High Speed Implementation of RSA Algorithm with Modified Keys Exchange [5].RSA is an asymmetric cryptosystem which is used to protect the information in order to provide confidentiality over the networks. To provide information security we apply RSA method in the network. In RSA algorithm speed of computation are slow. To speed up the process of algorithm a new offline RSA key generation method is provided. Here in this method to exchange the values of the keys between gateways. Gateways are exchange indexes refers to the fields that contain the values of public and private keys. Keys are store in the tables inside the database before starting the RSA algorithm to encrypt and decrypt the data, rather than using the exchange of real values n, e, and d. Keys are store in database using SQL server 2008. This method provides security but is still lengthy in computation.

Therefore to reduce the time complexity some concepts can be applied in order to improve its effectiveness.

Ishwarya M and Dr.Ramesh Kumar propose a novel method called Privacy Preserving Updates for Anonymous and Confidential Databases Using RSA Algorithm [1]. The privacy is an important issue in many applications such as medical research, data mining, intelligence research, cloud computing etc. This paper proposes a new concept to implement a real world anonymous database which improves the secure efficient system for protection of data, restricting the access to data even by the administrator thus maintaining the secrecy of individual patient. This technique applies in medical field in order to increase the security and efficiency. The limitation of this algorithm is it takes time to compute the results.

B.Persis Urbana Ivy, et al [9] proposed a novel method a modified RSA cryptosystem based on 'n' prime numbers. To secure information over the network. In this method they develop the existing RSA algorithm for using four prime numbers to factorize the large prime number. Prime numbers are used to provide more security in the network. The security of RSA is depends on factorization. The large prime numbers are not easily factorized. It proposes a modified RSA cryptosystem using 'n' prime numbers which is not easily breakable. This technique provides more efficiency and reliability over the network. The major drawback of this method is factorization. If the hacker factorizes the modulus n then whole RSA lock will be opened and from this keys are easily generated.

This proposed method is based on Research and importance of RSA cryptography algorithm in java[4]. This paper introduces the concept of RSA algorithm and presents the importance of RSA in java. Through this, they tried to improve and analysis the performance of RSA algorithm. They developed a piece of software for encrypt and decrypt the text files. According to this software, the time of encryption and decryption is shorter than the original RSA algorithm than those in java.security.* and java.crypto.*, it's far more convenient and flexible to combine it with other classes, especially IO ones. With this implementation, thus they are successfully developed a program for encrypting and decrypting text files. RSA class write in java is more practical and secure. Programmers could employ it in Java projects in need of RSA for encryption, decryption or digital signature.

3. Description of Proposed RSA Algorithm

A proposed RSA technique is based on existing RSA cryptography. In this scheme we developed a new algorithm which is based on modified RSA cryptosystem. For providing more security and increasing the speed of RSA, we implemented offline storage method in which the key parameters of RSA algorithm are stored in table which is identical in all network. All parameters which are used in RSA algorithm are stored before starts the algorithm. Here we use the index for transferring the public and private at the time of encryption and decryption of data between the networks. In this way we try to speed up the implement of proposed RSA method as compare to existing RSA technique. Here we maintain the table in matlab software and transfer index instead of actual keys for encryption and decryption. In proposed method we developed an algorithm which is based on modified RSA cryptosystem. Considering these assumptions for algorithm-

p , q, and r are prime numbers.
n is common modulus.
e is public key.
d is private key.
M is message.

3.1 RSA Proposed Method

1) Select the random values p, q, and r.
2) Calculate n=p*q*r.
3) Calculate Ø (n) = (p-1) (q-1) (r-1).
4) Calculate e such that gcd (e, Ø(n))=1 and 1<e<Ø(n).
5) Encrypt the message M where M<n and encrypt with public key e such that $C=M^e \bmod n$.
6) Decrypt the message M such that $M=C^d \bmod n$.

3.2 Offline Storage Method

In this paper security and speed of RSA algorithm are increased through offline storage of key parameters. RSA key pairs are stored in table which is identical in all networks.

idx	N	phi	D	E

Fig 1- Storage Table in Matlab

Idx-index
n-common modulus
e-public key
d- private key

All parameters which are used in RSA algorithm are stored before starting the algorithm. We use the third prime r thus if anyone want to hack the database table to guess the value of modulus n, he cannot get success because value of n depends on all three prime numbers n=p*q*r. Therefore it is hard to hack the table. Therefore it

is hard to hack the table simultaneously. We use the index which is placed along with the values of e, d, Ø (n) and n in table implements in matlab.

4. Implementation of Proposed RSA Cryptosystem

We implement our proposed RSA algorithm in Matlab software (R2012b).

- **Technique 1**:- This technique is the original RSA algorithm is implementing in Matlab software. In this method two prime numbers p and q are used.
- **Technique 2**:- This technique is based on original RSA algorithm but here we use the three prime numbers p, q and r instead of two (p & q).
- **Technique 3**:- This is the enhanced form of RSA algorithm based on offline storage of information. Through this method we minimize the encryption and decryption time as compare to original RSA algorithm.

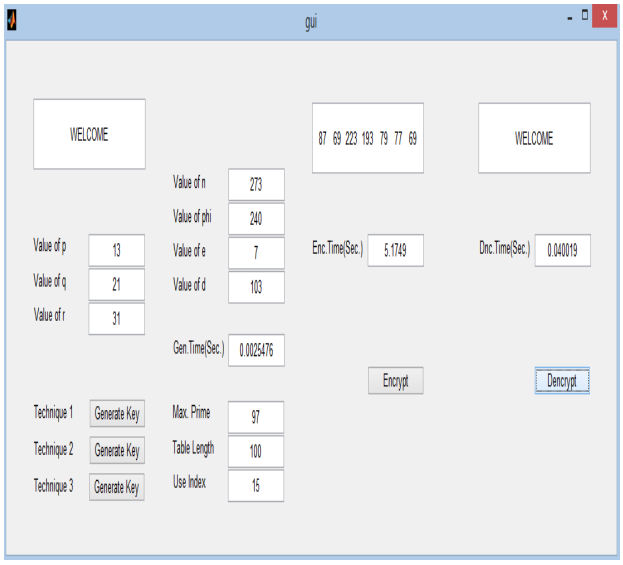

Fig 2- Graphical user Interface of Proposed RSA Cryptosystem.

5. Experiments and Results

With using RSA offline key generation algorithm and we calculate the encryption and decryption time of proposed RSA method for different values of prime numbers and also compare our proposed RSA method (Technique 3) with the original RSA algorithm (Technique 1).

Table 1- Search Time Analysis

ENCRYPTION / DECRYPTION TIME	TECHNIQUE 1	TECHNIQUE 2
ENCRYPTION TIME	4.67	4.59
DECRYPTION TIME	0.042	0.035
ENCRYPTION TIME	5.29	5.20
DECRYPTION TIME	0.031	0.040
ENCRYPTION TIME	6.04	6.10
DECRYPTION TIME	0.037	0.044
ENCRYPTION TIME	7.14	7.28
DECRYPTION TIME	0.058	0.055
ENCRYPTION TIME	6.78	7.05
DECRYPTION TIME	0.057	0.053
ENCRYPTION TIME	6.92	7.03
DECRYPTION TIME	0.055	0.059

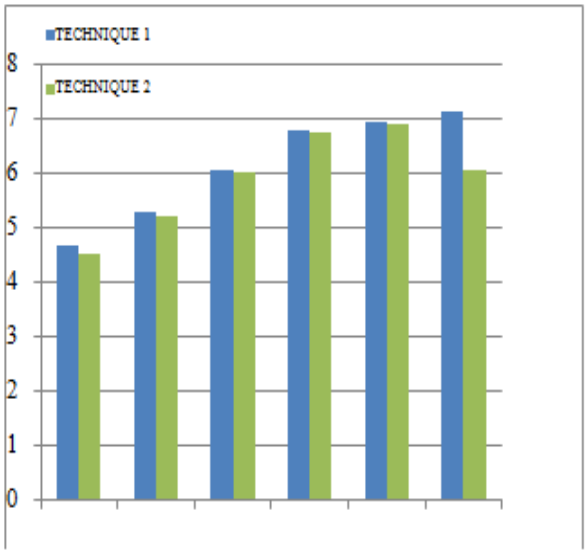

Fig 3- Graph shows comparison between encryption process using original RSA algorithm and offline proposed RSA method.

X-Axis:- Different values of p, q and r.

Y-Axis:- Encryption time (in seconds)

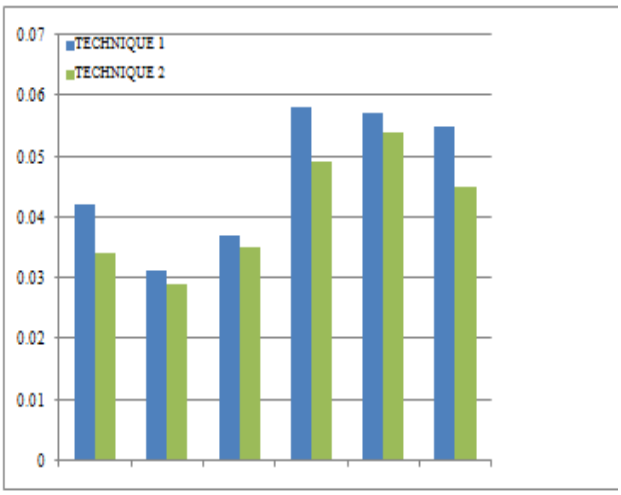

Fig 4- Graph shows comparison between decryption process using original RSA algorithm and offline proposed RSA method.

X-Axis:- Different values of p, q and r.

Y-Axis:- Decryption time (in seconds)

6. Conclusion

In this paper, we improve the security and increase the speed through the modification of an existing RSA algorithm called modified form of RSA algorithm based on offline storage and prime number. This paper contains the practical implementation of our proposed RSA algorithm using matlab software. This method use index to communicate instead of passing the actual values of public and private keys over the network, thus it provides more security as compare to an existing RSA method. In future some security concepts can be applied in the existing RSA algorithm for providing more efficiency and security.

Acknowledgment

The author wish to thank professor Rupali Bhartiya of Shri Vaishnav Institute of Technology & Science , Indore for her directive discussion in RSA cryptosystem.

References

[1] Ishwarya M, Dr. Ramesh Kumar. "Privacy Preserving Updates for Anonymous and Confidential Databases Using RSA Algorithm", International Journal of Modern Engineering Research (IJMER) , Vol.2, Issue.5, Sep.-Oct. 2012.

[2] Mandeep kaur and Manish Mahajan "Using encryption Algorithms to enhance the Data Security in Cloud Computing", International Journal of Communication and Computer Technologies Vol.01 – No.12, Issue.03, January 2013.

[3] Prof.Dr. Alaa Hussein Hamamiand, Ibrahem Abdallah Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm", International Conference on Advanced Computer Science Applications and Technologies, pp.402-408, Nov 2012.

[4] XinZhou and Xiaofei Tang "Research and Implementation of RSA Algorithm for Encryption and Decryption", The 6th International Forum on Strategic Technology, Vol.2, pp.1118-1121, Aug 2011.

[5] Sami A. Nagar and Saad Alshamma "High Speed Implementation of RSA Algorithm with Modified Keys Exchange", 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp.639-642, March 2012.

[6] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Vol. 21, pp.120-126, 1978.

[7] W. Stallings "Cryptography and network security", vol. 2 prentice hall, 2003.

[8] Ravi Shankar Dhakar and Amit Kumar Gupta "Modified RSA Encryption Algorithm (MREA)", Second International Conference on Advanced Computing & Communication Technologies, pp.426-429, Jan 2012.

[9] B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar "A modified RSA cryptosystem based on 'n' prime numbers", International Journal Of Engineering And Computer Science, Vol.1, pp. 63-66, 2 Nov 2012.

[10] Shilpi Gupta and Jaya Sharma "A hybrid encryption algorithm based on RSA and diffie hellman", IEEE International Conference on Computational Intelligence and Computing Research, pp.1-4, Dec 2012.

[11] Wuling Ren and Zhiqian Miao, "A hybrid encryption algorithm based on DES and RSA in Bluetooth communication", Second International Conference On Modeling, Simulation and Visualization Methods, pp. 221-225, May 2010.

[12] Sonal Sharma , Prashant Sharma and Ravi Shankar Dhakar "RSA Algorithm Using Modifiesd Subset Sum Cryptosystem", International On Computer and Communication Confrence Technology(ICCCT), pp. 457-461, Sep 2011

[13] Ashutosh Kumar Dubey ,Animesh Kumar Dubey , Mayank Namdev and Shiv Shakti Shrivastava "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", International Journal of Advanced Computer Research Vol.1, 2 December 2011.