Reformed RSA algorithm based on Prime Number

Raj J. Jaiswal
Assistant Professor
Department of Computer Engg.
RCPIT, Shirpur

Ranu Soni
Assistant Professor
Department of Computer Engg.
RCPIT, Shirpur

Prasad Mahale
Assistant Professor
Department of Computer Engg.
RCPIT, Shirpur

ABSTRACT
The most common public key algorithm is RSA cryptosystem used for encryption and decryption. It is the first public key algorithm which provides security to transfer and saving of data over the network. In RSA cryptosystem there is less security and time of computation is still lengthy. This paper suggest a new algorithm concept to presents the modified form of RSA algorithm in order to speed up the implementation of RSA algorithm during data exchange over the network. This includes the architectural design and enhanced form of RSA algorithm through the use of third prime number in order to make a modulus n which is not easily decomposable by intruders. A database system is used to store the key parameters of RSA cryptosystem before it starting the algorithm. Finally we compare proposed RSA method with the original RSA method by some theoretical aspects. Comparative results provide better security with proposed algorithm.

General Terms
Cryptography, Indexes, Public Key, Private Key

Keywords
RSA, RSA protocol, Offline Storage, Prime Number

1. INTRODUCTION
Today's world it should be noted that all works are related to banking, ATM card, credit card, marketing, Ecommerce etc are doing with the help of internet. So there must be security provided over the network. Therefore for secure communication we have many cryptography techniques such as hash function, diffie Hellman algorithm, digital signature, message authentication code, MD5 algorithm, Rabin cryptosystem and RSA cryptosystem etc. We apply these techniques to secure information in order to provide confidentiality from an unauthorized access. Large volume of personnel and sensitive information are electronically transmitted and stored every day. In cryptosystem data are secured through encryption method for making communication private. Anyone send the private message by encrypting the message and intended receiver decrypts it by its key [7]. It uses the identical database over the network. We store the parameters of RSA algorithm in a database table before starting the RSA method to encrypt and decrypt. We use index value to exchange rather than original values of e and d. In this paper we consider theoretical aspects and compare our proposed method with existing algorithm [4].

In proposed method we add some concepts of existing RSA method in order to provide better security. Let's consider how keys are generated in RSA cryptosystem.

1.1 RSA Methodology
RSA cryptosystem is one of the famous security algorithms which is composed of three phases: key generation, encryption process and decryption process.

1.1.1 Key Generation
a) Select p and q both prime number, p is not equal to q.

b) Calculate n = p x q.

c) Calculate ø (n) = (p -1) x (q-1).

d) Select integer e whose gcd (Ø (n), e) = 1; 1 < e <Ø (n).

e) Calculate d = e-1 (mod Ø (n)).

f) Public key PU = {e, n}.

g) Private Key PR = {d, n}.

1.1.2 Encryption Process
a) Plaintext- Message (M)

b) Cipher text- $C = M^e \bmod n$.

1.1.3 Decryption Process
a) Cipher text- C

b) Plaintext- $M = C^d \bmod n$.

Where M is message, p and q are prime numbers. N is common modulus. e and d are public and private keys.

1.2 Importance of RSA Method
RSA is one of the famous security cryptosystem based on number theory. RSA method ensures the information are confidential and authenticated, thus it provides secure communication over the network. Its security is based on the difficulty in factoring very large numbers. Based on this principle, the RSA encryption uses prime factorization as the trapdoor for encryption. It uses public key encryption in which anyone use public key to encrypt the data and send over the network. Its provides authentication and security over the network in order to provide private key to decrypt the information therefore only indented receiver can decrypt the information. RSA algorithm is used for both data encryption and digital signature.

1.3 Limitation in RSA Algorithm
The limitation of using public key cryptography for encryption and decryption is speed. Its computation takes time to compute the mathematical operation of RSA algorithm. Public key is used for encryption should be authenticated. If hacker knows the factors of a large prime number then this break the security of algorithm, because the values of p, q, d, and e are known with the help of factors. loss of private key may be leak the information in the communication network.

2. LITERATURE REVIEW
Shilpi Gupta and Jaya Sharma proposes a joint method 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. 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 establish 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). In knapsack problem, given a list of third number which is the sum of a 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 refer 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 provide 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 proposes a novel method called Privacy Preserving Updates for Anonymous and Confidential Databases Using RSA Algorithm [2]. 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. proposed a novel method a modified RSA cryptosystem based on 'n' prime numbers [9]. To secure information over the network, this method develops 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 key are easily generated.

3. PROBLEM DEFINITION

RSA algorithm works slowly and provides less security over the `network. To increase the speed of computation of RSA algorithm and to increase the security we need to modify the RSA algorithm which can be done by third prime number and offline storage method.

4. PROPOSED METHOD

In proposed method we developed an algorithm which is based on modified RSA cryptosystem [8]. Considering these assumptions for algorithm-

a) p, q, r and s are prime numbers.

b) n is common modulus.

c) e is public key.

d) d is private key.

e) M is message.

4.1 RSA Proposed Method

a) Select the random values of p, q, r, and s.

b) Calculate n=p*q*r*s.

c) Calculate Ø (n) = (p-1) (q-1) (r-1)(s-1).

d) Calculate e such that gcd (e, Ø (n)) = 1 and 1 < e < Ø (n).

e) Encrypt the message M where M< n and encrypt with public key e such that $C=M^e$ mod n.

f) Calculate private key such that e*d=1mod Ø (n).

g) Decrypt the message M such that $M=C^d$ mod n.

4.1.1 Offline Storage Of public and private key

In this paper security and speed of RSA algorithm are increased through offline storage of key parameters. RSA key pairs are stored in database which is identical in all networks. All parameters which are used in RSA algorithm are stored before starting the algorithm. There are two tables inside a database engine to save the keys. First table contain the values of p, q, N1, Ø (N). Second table contain the values of e, d, r, s, E1, D1.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*s. Therefore it is hard to hack both the table simultaneously.E1 and D1 are the indexes of public and private key. p, q and r are three prime numbers. e and d are actual public and private keys.

4.1.2 Key exchange

Key is exchange from sender to receiver by using database which is stored on the cloud or on network . As shown on fig 2 sender fetch the value of e1 and n1 from the database instead of the actual values of e, n and e1, n1 show the index value of e, n . similarly receiver fetch the values of d1 (index value of d), and n1 (index of value of n) from the database instead of actual value.

4.1.3 Encryption and Decryption Process

As shown in fig 2 Encrypt the message by using public key (e1, n1) and send to the receiver and receiver decrypt the message which is send by the sender by using private key (d1, n1).

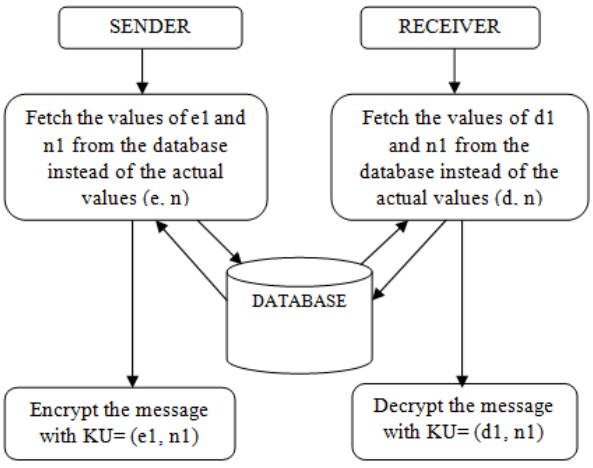

Fig.2- Architecture of Proposed RSA

5. CONCLUSION

In proposed method keys are stored offline before the process starts, thus increasing the speed of process as compared to original RSA method. If an unauthorized person wants to wants to know the value of p, q and r from the two database tables. It is difficult to guess the value of p, q and r simultaneously from the database. This method provides more security and it is reliable to use in networks and cloud computing environment. We worked on security and speed by providing offline storage method with the use of three prime numbers instead of two prime numbers as in RSA algorithm. In future some security concepts can be applied in the existing RSA algorithm for providing more efficiency and security.

6. 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) www.ijmer.com 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 Communicationand Computer Technologies Volume 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, March2012.

[6] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," vol. 21 (2), 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", ISSN:2319-7242 Volume1 Issue Page No. 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 Researc, 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 Modifiend Subset Sum Cryptosystem", International Confrence On Computer and Communication Technology(ICCCT), pp. 457-461, Sep 2011.

[13] Ashutosh Kumar Dubey ,Animesh Kumar Dubey , Mayank Namdev, 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 Volume 1 Number, 2 December 2011.

[14] Amanjot Kaur, Manisha Bhardwaj,"Hybrid Encryption Security For Cloud Database Security", International journal Of Engineering Science And Technology ISSN No:2250-3676 Volume 2, May-June 2012.

[15] Li Dongjiang, Wang Yandan, Chen Hong, "The research on key generation in RSA public- key cryptosystem", Fourth International Conference on Computational and Information Sciences, pp. 478-480, Aug 2012.

[16] Rajani Devi.T, "Importance of Cryptography in Network Security",International Conference on Communication Systems and Network Technologies, 2013.

[17] Aayush Chhabra, Srushti Mathur," Modified RSA Algorithm", International Conference on Computational Intelligence and Communication Systems, 2011.

[18] Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7, July 2012.

[19] Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, September 2012.

[20] Ping Yu, Stephen R. Tate," An Online/Offline Signature Scheme Based on the Strong RSA Assumption", 21st International Conference on Advanced Information Networking and Applications Workshops, Vol 1, pp. 601-606, May 2007.

[21] Evgeny Milanov, "The RSA algorithm", June 2003.

[22] N. Saravanan, A. Mahendiran, et al,"An Implementation of RSA Algorithm in Google Cloud using Cloud SQL" , Research Journal of Applied Sciences, Engineering and Technology, Oct 2012.

[23] Paul C. Kocher, "Timing Attacks on Implementations of De-Hellman", RSA, DSS, and Other Systems", pp.1-10.

[24] Kumarjit Banerjee, Satyendra Nath Mandal, Sanjoy Kumar Das, "Improved Trial Division Technique for Primality Checking in RSA Algorithm", July 2013.

[25] J. Joshi, et al. "Network Security", Morgan Kaufmann, 2008.

[26] W. Stallings "Network and internetwork security: principles and practice", Prentice-Hall, Inc., 1995.

[27] Himani Agrawal and Monisha Sharma," Implementation and analysis of various symmetric cryptosystems" Indian Journal of Science and Technology, Dec 2010.

[28] W. Stallings "Network security Essentials: Applications and Standards", Pearson Education India, 2000.

[29] R. L. Rivest, A. Shamir and L. Adleman "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 1978.EEE Standard Specifications for Public-Key Cryptography, 2000.