A Survey and Performance Analysis of Various RSA based Encryption Techniques

Sarika Khatarkar
M. Tech. Scholar
Technocrats Institute of Technology, Bhopal,
Madhya Pradesh, India

Rachana Kamble
Asst. Professor
Technocrats Institute of Technology, Bhopal,
Madhya Pradesh, India

ABSTRACT
Network and Internet applications are growing very fast, since the need to secure these applications are very fast. So the importance and the value of the swapped data by the internet and other media types are increasing. The protection of multimedia data, sensitive information like credit cards, banking transactions and social security numbers is becoming very important. For secure transmission of data in open network, encryption is very important methodology. In recent years many encryption methods have been proposed and used to protect confidential information. In this survey paper many different asymmetric cryptography techniques, like RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm) are analyzed. Also discussed many other efficient algorithms.

Keywords
RSA, i-RSA

1. INTRODUCTION
For security and speed of RSA, it has some important parameters. By increasing the modulus length it plays an important role for increasing the complexity of decomposing it into its factors. That increases the length of private key and hence it will difficult to be decrypted without knowing the decryption key. Length of encrypted message proportionally changes when the message length is changed.

hence to obtained larger encrypted message, larger size chunks are selected to increase the security of the data in use[10]. An organization with suffientely deep pockets, It is possible that can build a large scale version of his circuits and effectively crack an RSA 1024 bits message in a relatively short time period, which could range anywhere from a number of minutes to some days[7,8]. Performance of RSA algorithm analyzed by varying that parameters with respect to time[9]. For pair of keys, we use natural numbers, in addition to existing parameters of RSA. Then after simulations of results on basis of speed and security we compare the new algorithm and RSA.

RSA Key Generation, Encryption, Decryption Process

The following steps are there to determine the values of e, d and n.

- Choose two very large (100+ digit) prime numbers p and q.
- Set n equal to p * q.
- Choose any large integer, e, such that

GCD (e, ((p-1) * (q-1)) = 1

- Find d such that e * d mod ((p-1)*(q-1)) = 1

The public key is the number (n, e). Although these values are publicly known, it is computationally infeasible to determine 'd' from 'n' and 'e' if p and q are large enough. To encrypt a message, M, with the public key, creates the cipher, C, using the equation:

C = Me mod n e: Public Key

The receiver then decrypts the cipher with the private key using the equation:

M = Cd mod n d: Private Key

Now, this might look a bit complex and, indeed, the mathematics does take a lot of computer power, given the large size of the numbers; since p and q may be 100 digits (decimal) or more, d and e will be about the same size and n may be over 200 digits.

Nevertheless, a simple example may help. In this example, the values of p, q, e and d are purposely chosen to be very small and the reader will see exactly how badly these values perform, but hopefully the algorithm will be adequately demonstrated.

2. LITERATURE SURVEY
2.1 Modified RSA based on Multiple Public Keys
security is required to transmit confidential information over the network, in the today's world. In wide range of applications, Security is also demanding. For data security Cryptographic algorithms play a vital role against malicious attacks. In the popular implementations of Public Key Infrastructures, RSA algorithm is extensively used. this paper[1] an algorithm is proposed for RSA a method for implementing a public-key cryptosystem (RSA) using two public key and some mathematical relation. This two public keys are sent separately, this makes the attacker not to get much knowledge about the key and unable to decrypt the message. The proposed RSA[1] is used for system that needs high security. but with less speed. Two different keys are used in Public Key cryptography. One key is used for decryption & only the other corresponding key must be used for encryption. Not any other key is possible to decrypt the message, even the original (i.e. the first) key can't used for encryption. Every communicating party needs just a key pair for communicating with any number of other communicating parties. It is beauty of this scheme. Once someone obtains a key pair, he /she can communicate with anyone else. They have done implementation of RSA algorithm efficiently using two public key pairs and using some mathematical logic rather than sending the e value directly as a public key. Because if an attacker has opportunity of getting the e value they can directly find d value and decrypt the message.

2.2 Personal Information Protection Approach Based on RSA
with the rapid development and widespread application of the information technology, the communication pattern has obviously changed between individuals, corporations and

even nations. However, convenient network-based communication method brings not only the benefits but also some disadvantages such as personal information leak. this paper[2] introduced a new personal information protection approach based on RSA cryptography. With this approach, personal information can be transformed from plain text into cipher text. Customer representatives will be able to contact their clients without seeing the privacy. On the server side, the system administrator has the permission of authorization management. They devolve the authorization to database administrators and then database administrators input customers' information into the system. At the same time, sensitive information such as phone number is encrypted. On the client side, the customer representatives only see the names list.

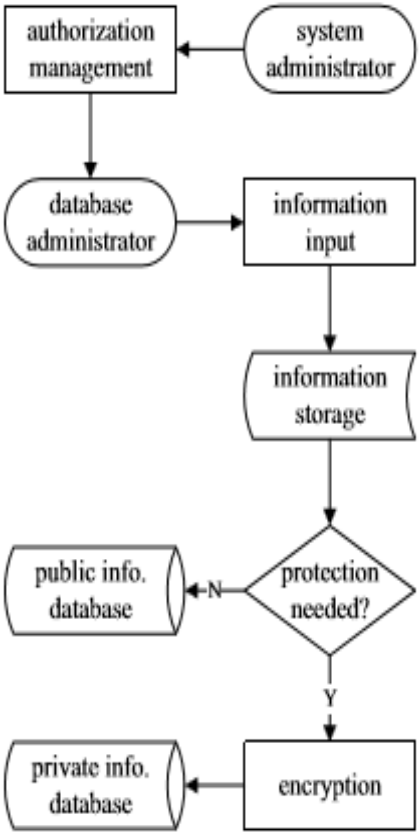

Figure 2. The encryption approach of customers information

When operation is needed, software installed on the customer representatives' computer or cell phone will decrypt the data and send them to the call center directly without touching the representatives.

2.3 Quantum Key Distribution

using the current computing systems classical cryptography is based on the computational difficulty to compute the secret key. Depending only on the difficulty of computational complexity does not provide enough security because finding a fast method to calculate the secret key. it will compromise the security of the systems. Law of physics is used in Quantum computing for communication. In cryptography and key distribution quantum theorems and principles are applied. In this paper[3], new model for quantum key distribution are introducing among three parties or more where there is a trusted center that providing the clients necessary secret information to securely communicate with each other.

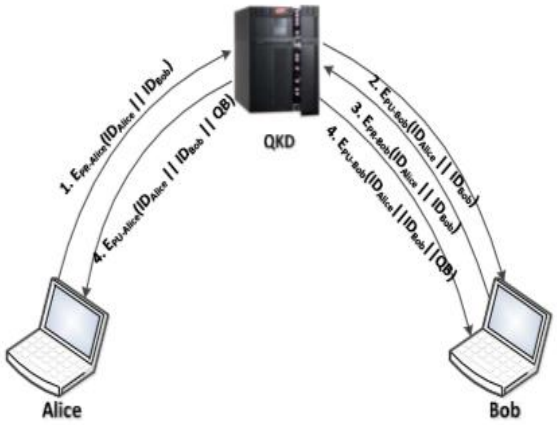

Figure 3. User Authentication and Quantum Bases distribution

Quantum key distribution protocols BB84, B92 and EPR communicate using a classical channel to compare the bases. This approach facilitates eliminating the erroneous qubits. They introduce a novel security quantum algorithm that employs public key encryption algorithm to generate keys to improve security over quantum communication channel. Moreover, the introduced algorithm enhances user's authentication and data privacy.

2.4 i-RSA Algorithm

This paper[4] propose i-RSA algorithm, that is focus on key generation algorithm. user identity is Enhancement of this algorithm. it can be used as a public key, such as email address. The key certificates are used to authenticate the user's key pair. So certificate does work as important role in secure communication but to issue the certificate is a big challenge and it also increases the overhead due to the increasing cost. For public key Previous algorithm was successful used email identity, but all type of email can't be used as a public key. So the propose i-RSA algorithm that can produces 66.6% compared to previous algorithm (46.67%) email can be a string public key. in key generation looping process is the main differences between i-RSA and previous algorithm, to get new value of p and q parameter, when value of k is equal to 1, then looping process will stop, and the email can be a public key. Detail explanations of i-RSA algorithm in propose algorithm section..

2.5 Modified RSA Cryptosystem Based on Offline Storage and Prime Number

In RSA cryptosystem there is less security and time of computation is still lengthy. This paper[5] 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 across 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. In this method keys are stored offline before the process start. Thus, the speed of process increased as compared to original RSA method. The proposed RSA method is compared with the original RSA method by some theoretical aspects. Comparative results provide better security with proposed algorithm.

2.6 Enhancing the Security of the RSA Cryptosystem

This paper[6] increases the security of the RSA algorithm, this enhancement use randomized parameter to change every encrypted message block such that even if the same message is sent more than once the encrypted message block will look different. This paper suggests that how to use randomized parameters in the encrypt the data to make RSA. By this enhancement it makes the RSA semantically more secure. Means an attacker cannot distinguish two encryptions from each other, even if the attacker knows (or has chosen) the corresponding plaintexts(original message). In this paper a comparison between the modified RSA and the basic RSA version introduced. Enhancement can easily be implemented on this paper. Also other attacks are presented by this paper, also how to speed up the RSA encryption and decryption process is an important issue for the RSA implementation.

Table 1 Algorithms based on RSA

S. No.	Authors	Algorithm	Year	Uniqueness
1	Amare Anagaw Ayele, Dr. Vuda Sreenivasarao	Modified RSA Based on Multiple public keys	2013	using two public key's and sent separately.
2	Liang Wang, Yonggui Zhang	Personal Information Protection Approach Based on RSA	2011	At the same time, sensitive information such as phone number is encrypted.
3	Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah,	Quantum Key Distribution	2013	introduce a novel security quantum algorithm that employs public key encryption algorithm to generate keys to improve security over quantum communication channel.
4	Norhidayah Muhammadi, Jasni Mohamad Zaini, Md Yazid Mohd Saman	i-RSA algorithm	2013	user identity can be used as a public key such as email address. And using looping process in key generation, to get new value of p and q parameter.
5	Ms. Ritu Patidar, Mrs. Rupali Bhartiya	Modified RSA Cryptosystem Based on Offline Storage and Prime Number	2013	It uses 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 starts the algorithm.
6	Malek Jakob Kakish	Enhancing The Security Of The RSA Cryptosystem	2011	It uses randomized parameter to change every encrypted message block such that even if the same message is sent more than once the encrypted message block will look different.

3. CONCLUSION

Cryptography plays vital role in explosive growth of digital data storage and communication. In this paper, it has been surveyed that the existing works on the RSA encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. The various cryptanalysis attacks including passive and active attack can break the cryptosystem. The attacker can used modulus operator to break the RSA algorithm. The main purpose of this paper is to disseminate the basic knowledge about the RSA based algorithms and comparison of available RSA based encryption techniques based on some parameters like vulnerability to attack, Uniqueness about the technique, etc. and here we have seen that RSA is more secure and it may be more stronger by applying some techniques. Here we have seen that all authors are talking about many method but no one is talking about image pixel for security purpose. So we can add image pixel technique to make more powerful RSA algorithm.

4. REFERENCES

[1] Amare Anagaw Ayele, Dr. Vuda Sreenivasarao, June 2013, "A Modified RSA Encryption Technique Based on Multiple public keys", International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 4.

[2] Liang Wang, Yonggui Zhang, 2011, "A New Personal Information Protection Approach Based on RSA Cryptography", IEEE.

[3] Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah, 2013, "Quantum Key Distribution by Using Public Key Algorithm(RSA)", IEEE.

[4] Norhidayah Muhammadi, Jasni Mohamad Zaini, Md Yazid Mohd Saman, "Loop-based RSA Key Generation Algorithm using String Identity", 13th International Conference on Control, Automation and Systems (ICCAS 2013).

[5] Ms. Ritu Patidar, Mrs. Rupali Bhartiya, 2013, "Modified RSA Cryptosystem Based on Offline Storage and Prime Number", IEEE.

[6] Malek Jakob Kakish, "Enhancing The Security Of The Rsa Cryptosystem", Ijrras August 2011.

[7] KetuFile White Papers "Symmetric vs. Asymmetric Encryption ", a division of Midwest research corporation.

[8] RSA Laboratories : Technical Notes and Papers.

[9] A fast implementation of the RSA algorithm using the GNU MP library. By Rajorshi Biswas,Shibdas Bandyopadhyay,Anirban Banerjee, IIIT – Calcutta.

[10] Sensitivity of Changing the RSA Parameters on the Complexity and Performance of the Algorithm By Allam Mousa ;Journal of Applied Science 5 (1) :60-63,2005 ISSN 1607 – 8926.Asian Network for Scientific Information.