International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 7 163 - 168

Survey and Idea of Enhancement over Various RSA based Cryptographic Techniques

Shikha Mathur
Masters of Technology, Student
MEC, Bikaner
shikhamathur806@gmail.com

Deepika Gupta
Assistant Professor, Guide
MEC, Bikaner
deepika.gupta1218@gmail.com

Abstract: Internet and its applications are growing very fast, since the need to secure these applications are very fast. For secure transmission of data over network, encryption is very important methodology. This cause a major concern for privacy and security etc. cryptography is a standard way to secure the data over the medium. In a distributed network, when information has to be send over network, cryptography become important part of secure communication. Cryptography has been developed from the Greek word krypto and graphin which means is hiding information from unauthorized person. In recent years various encryption decryption methods have been proposed and used to protect confidential information. In this survey paper various RSA based techniques are studied and described. This paper includes the survey of the work done by various researchers in the field of cryptography and idea about modified approach.

Keywords*: Public Key, Private Key, RSA, RSA protocol, Symmetric Key and Asymmetric Key, 'n' prime number, multiple public key*

*****

I. INTRODUCTION

In today's era, internet is the basic necessity for communication between people and facilitates for electronic payment, military communication and many other secret communications. This cause a major concern for privacy and security etc. cryptography is a standard way to secure the data over the medium. Cryptography has been developed from the Greek word crypto and graphy which means is hiding information from unauthorized person and the person who study and discover cryptography are called cryptographers and study of cryptography is defined as cryptanalysis. Cryptography is a part of secret information, it is technique for protecting the information over the medium. It is process of converting readable text to unreadable text. In a distributed network, when information has to be send over network, cryptography become important part of secure communication [1].

II. LITERATURE REVIEW

This section involves the work done by various researchers in the field of cryptography.

[1] M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya, proposed an enhanced RSA approach. They proposed an approach which includes four prime numbers instead of two prime numbers thereby maximizes the time for intruders needed to guess these primes. The calculation of public key 'E' and private key 'D' depends on the value of N, which is the product of prime numbers. As a result the key generation time of proposed algorithm is more than traditional RSA and other compared RSA. Higher the key generation time, higher the time needed to break the system, thereby making the system strong [1].

Limitation - The encryption and decryption time of proposed approach is higher than original RSA.

[2] Zhenjiu Xiao, Yongbin Wang, Zhengtao Jiang, proposed a modified form of RSA digital signature algorithm. They proposed a four-prime Chinese remainder theorem digital signature algorithm in this paper. They used the Hash function SHA512 to make message digest. They optimized large number modular exponentiation with CRT combining in Montgomery algorithm. They used four primes CRT-RSA signa-

ture algorithm, which combines with Montgomery modular exponentiation algorithm and the Chinese remainder theorem to make the process of signature efficient [2].

Limitation - Proposed approach is vulnerable to chosen-cipher text attack.

[3] Xianmeng Meng, Xuexin Zheng, they analyze short exponent RSA with a small parameter *k*. They show tha birthday attack may cause this RSA variant insecure. This improves the former result [3].

Limitation - Proposed approach is more complex and time consuming.

[4] Sangita A. Jaju, Santosh S. Chowhan, presents a comparison between RSA and Modified RSA algorithm along with time and security by running several data test to check data of different sizes. The efficiency of these algorithms was based on key generation speed. The texts of different sizes were encrypted and decrypted using RSA and modified RSA algorithms [4].

Limitation - Time complexity is increased and in terms of encryption and decryption speed traditional RSA is better.

[5] Dr. D.I. George Amalarethinam, J.Sai Geetha, proposed an additional level of security using single magic rectangle. By using it they enhances the randomness of the calculated cipher text. In the existing work, repetition of encrypted text takes place when the characters are repeated in the original text because of ASCII value. In Magic rectangle, there will be no repetition of values. Even if the repetition of same character takes place, magic rectangle assigns different value for every single occurrence of that same character. By doing this, it is difficult for attacker to guess the information which is being transmitted over network [5].

Limitation – In proposed approach additional time is needed for the construction of magic rectangle.

[6] Aswathy B.G, Resmi R, presents two architectures for implementation of modular exponentiation algorithm. In the first stage two mapping operations are performed with two multipliers. In the second stage of this performing the square and multiplication operation that is the stage where modular multiplication is done [6].

Limitation – Original RSA has better performance than this proposed approach.

[7] Rohit Minni, Kaushal Sultania, Saurabh Mishra, Prof Durai Raj, presents a modified algorithm of RSA with enhanced security. The new security feature introduced is the removal of n (product of two prime numbers) from the original RSA algorithm. Instead, the newly generated value which replaces n can be used in both the public key and private key. The algorithm presented in this paper eliminates factorization attack issue and makes the algorithm more secure with a slight increase in time complexity [7].

Limitation - In proposed algorithm time complexity is increased.

[8] Prof.Dr.Alaa Hussein Al-Hamami, Ibrahem Abdallah Aldariseh, presents enhanced RSA algorithm through the use of additional third prime number in addition of public and private key. This will increase the factorization complexity of n (product of prime numbers). They use three prime numbers with reduced size, generates large variable n and the process of factorization is more difficult than the original algorithm, as well as, increases the ease of generating Public and private key. In this case it is very difficult for the intruder to find the values from factoring n [8].

Limitation - In proposed approach complexity increases.

[9] Ms. Ritu Patidar1, Mrs. Rupali Bhartiya, introduces a new concept to present the modified approach of existing RSA algorithm in order to decrease time complexity of the RSA algorithm during communication over the network. This includes enhanced form of RSA algorithm through the use of additional third prime number so that modulus n is not easily divisible by intruders. It includes database which stores the key values of RSA cryptosystem before it starts. In proposed method keys are stored already before the process start. Thus,

the speed of encryption decryption increases as compared to traditional RSA method [9].

Limitation - Proposed approach uses database which can be hacked easily.

[10] Li Dongjiang, Wang Yandan, Chen Hong, presents the generation of prime numbers and the public and private key. Existing way of generating a prime number is more time-consuming, to resolve such problem, an improved algorithm is introduced. As a result, it improves the efficiency of prime number and key generation. After the introduction of Stain algorithm, the encryption and decryption time is noticeably shortened [10].

Limitation - More complex than original RSA.

[11] Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma, and presents a cryptography algorithm which is a combination of homomorphic properties called Modified RSA Encryption Algorithm. Modified RSA is more secure as compared to traditional RSA as it is based on the factoring problem. The scheme is an additive homomorphic cryptosystem; which means that, if the public-key and the encryption of m1 and m2 is given, one can compute the encryption of m1 + m2 [11].

Limitation - Proposed approach decreases the speed of encryption, decryption and key generation.

[12] Sami A. Nagar, Saad Alshamma, proposed a new approach of keys exchange between the sender and receiver to increase the difficulty for intruder to guess these exchanged values n, e and d. They called this approach Indexes exchange, and speedup the RSA algorithm by developing a new key generation method called RSA-key generation. Generates keys offline and save all key values in database tables. They proposed four level security, each level has its own database and collection of sets, these levels identified according to the values of e and key length, before start using the RSA algorithm between sender and receiver, must get a Ready Acknowledgment from RSA Handshake Database, and this protocol is responsible for updating the identical gateways database, level selections and establishing the algorithm between gateways [12].

Limitation - It uses database, easily can be attacked by intruders.

[13] Shilpi Gupta, Jaya Sharma, proposed an approach by mixing the two most popular algorithms RSA and Diffie-Hellman in order to enhance more security. RSA algorithm is a Public key cryptography method, based on Prime Numbers. Its security feature is based on the difficulty of factoring product of large prime numbers. Whereas, Diffie Hellman algorithm used for key exchange method that allows two communicating parties that have no prior knowledge of each other to share a secret key. In this paper they use both RSA and Diffie- Hellman for providing more security [13].

Limitation - In proposed approach time complexity should be revised for better working of algorithm.

[14] Aayush Chhabra, Srushti Mathur, proposes a new modified and secured approach than traditional RSA algorithm, which is used for both digital signatures and encryption-decryption. Proposed method removes the need to transfer n, the product of two random prime numbers, in the public key cryptosystem due to which it becomes difficult for the intruder to decompose n and hence the encrypted data remains safe from the intruders. Thus in this way this approach provides a more secured way for transmission of information using public key cryptography [14].

Limitation - Increase in complexity.

[15] Xin Zhou, Xiaofei Tang, presents a complete discussion of the cryptography, encryption, decryption, and RSA public key and other related technology applications in the military, business, privacy and other fields of information security which plays an important role. Problem for RSA encryption on the file, it indicates the RSA mathematical algorithms in the computer industries importance and its shortcomings. It discusses the questions of how to apply to the personal life of RSA information security issues. And also contains the use of

RSA and the basic principles of data encryption and decryption. In the end, they proposed a new program to improve RSA algorithm based on RSA cryptography and the extensive application [15].

Limitation - Complexity increases in proposed approach.

[16] Dr. Abdulameer K. Hussain, presents an effective solution to enhance the security of traditional RSA scheme. The objective of this proposed method is when RSA is implemented, there is a situation in which the encrypted text (cipher text) is the same as the plain text (original text) in some values of n (product of two prime numbers). So it is very important to find an effective solution for such a problem because it is vulnerable for most common attacks. In order to resolve such problem, the proposed method introduce a new method to change the value of n by forming a large set of prime numbers from which the users can select values of either one prime number or both used for changing the value of n and to ensure more security [16].

Limitation - Change in distance again and again to maintain security.

[17] Ritu Tripathi, Sanjay Agrawal, presents survey on RSA algorithm and various Improved RSA algorithm. RSA is highly secured algorithm but have more computation time and slow speed, so various techniques are proposed to increase the speed of an existing RSA algorithm by applying various modification in original RSA. This paper is about the detailed study of various techniques and represents the summarized results [17].

[18] Raj J. Jaiswal, Ranu Soni, Prasad Mahale, presents a new concept to presents the modified RSA algorithm such that to increase speed of encryption and decryption over traditional RSA algorithm during data exchange over the network. In proposed method keys are stored offline before the process starts, thus increasing the speed of process as compared to original RSA approach, if an unauthorized person wants to know the value of p, q and r from the database table. It is difficult to guess the value of p, q and r simultaneously from the database. This method provides more security and reliable to use for data transmission over the networks [18].

Limitation - Offline storage before the process starts, some security measures should be added.

[19] Akansha Tuteja, Amit Shrivastava, presents implementation of RSA encrypt/decrypt solution based on the study of RSA public key algorithm, they use RSA algorithm for digital signature. Digital signature proves the authenticity of a digital document. If digital signature is valid at receiver's side then it proves the recipient to trust that the message was created by an authorized sender and during transformation, it was not altered by any other person. In their proposed approach, encryption and decryption of message is faster and more secure against common module attack as compared to existing RSA cryptosystem. Also the proposed approach is more safe and secure against low decryption exponentiation attack, because we are using a large value of d [19].

Limitation - Less secure than existing RSA.

[20] Amare Anagaw Ayele, Dr. Vuda Sreenivasarao, proposes a new RSA approach which includes two public key. These two public keys are sent separately, so that the attacker not to get the idea and those systems that needs high security but with less speed in those this approach can be used. The main idea of this scheme is that every communicating party needs just a key pair for communicating with any other communicating party. Once someone obtains a key pair, he /she can communicate with anyone else [20].

Limitation - High security but less speed.

III. IDEA OF MODIFIED APPROACH

After analysis of previous work done on RSA cryptographic approach I come to the conclusion to overcome some of the limitations of previous work. In future I will modified the traditional RSA approach by including four prime numbers to avoid factorization attack, multiple public keys which are sent separately to increase security, and will apply a approach called K-NN to solve the redundancy problem of cipher text to make it more secured and also apply some verification

code to both sides sender and receiver, to maintain the integrity and authenticity of message and increase the complexity of the approach. I will apply the modified approach on images, text messages and special characters to increase security feature and in future will apply the same to audios and video files also.

IV. CONCLUSION

Cryptography plays an important role in this digital world. Cryptography is a part of secret information, it is technique for protecting the information over the medium. It is process of converting readable text to unreadable text. In a distributed network, when information has to be send over network, cryptography become important part of secure communication. In this paper there is a survey of existing work on RSA encryption techniques. These techniques are studied and performance of encryption methods also studied.

From the above survey it is clear every author is talking about security, key generation, attacks, but, no one is talking about image security. So we can add image security in existing RSA techniques to make it more effective.

V. REFERENCES

[1] M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya, "An Enhanced and Secured RSA Key Generation Scheme", Department of Information Technology, Anna University, Chennai, 2214-2126/© 2014, Elsevier.

[2] Zhenjiu Xiao, Yongbin Wang, Zhengtao Jiang, "Research and Implementation of Four-prime RSA Digital Signature Algorithm", Las Vegas, USA, 978-1-4799-8679-8, 28-July 2015, IEEE.

[3] Xianmeng Meng, Xuexin Zheng, "Cryptanalysis of RSA with a small parameter revisited", Information Processing Letters 115-2015, 858-862, Elsevier.

[4] Sangita A. Jaju, Santosh S. Chowhan, "A Modified RSA Algorithm to Enhance Security for Digital Signature", 978-1-4799-6908-1/15/©2015, IEEE.

[5] Dr. D.I. George Amalarethinam, J.Sai Geetha, "Enhancing Security level for Public Key Cryptosystem using MRGA", World Congress on Computing and Communication Technologies, 978-1-4799-2876-7/13/, 2014, IEEE.

[6] Aswathy B.G, Resmi R, "Modified RSA Public Key Algorithm", First International Conference on Computational Systems and Communications (ICCSC), 978-1-4799-6013-2/14- 2014, IEEE.

[7] Rohit Minni, Kaushal Sultania, Saurabh Mishra, Prof Durai Raj, "An Algorithm to Enhance Security in RSA", 4th ICCCNT 2013, IEEE.

[8] Prof. Dr.Alaa Hussein Al-Hamami, Ibrahem Abdallah Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm", International Conference on Advanced Computer Science Applications and Technologies, 978-0-7695-4959-0/13, 2013, IEEE.

[9] Ms. Ritu Patidar1, Mrs. Rupali Bhartiya, "Modified RSA Cryptosystem Based on Offline Storage and Prime Number", International Conference on Computational Intelligence and Computing Research, 978-1-4799-1597-2/13, 2013, IEEE.

[10] Li Dongjiang, Wang Yandan, Chen Hong, "The research on key generation in RSA public- key cryptosystem", Fourth International Conference on Computational and Information Sciences, 978-0-7695-4789-3/12, 2012, IEEE.

[11] Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma, "Modified RSA Encryption Algorithm (MREA)", Second International Conference on Advanced Computing & Communication Technologies, 978-0-7695-4640-7/12, 2012, IEEE.

[12] Sami A. Nagar, Saad Alshamma, "High Speed Implementation of RSA Algorithm with Modified Keys Exchange", 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications, 978-1-4673-1658-3/12, 2012, IEEE.

[13] Shilpi Gupta, Jaya Sharma, "A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman", International Conference on Computational Intelligence and Computing Research, 978-1-4673-1344-5/12, 2012, IEEE.

[14] Aayush Chhabra, Srushti Mathur, "Modified RSA Algorithm A Secure Approach", International Conference on Computational Intelligence and Communication Systems, 978-0-7695-4587-5/11, 2011, IEEE.

[15] Xin Zhou, Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", 6th International Forum on Strategic Technology, 978-1-4577-0399-7/111, 2011, IEEE.

[16] Dr. Abdulameer K. Hussain, "A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2, Issue 1, ISSN 2348-7968, January 2015.

[17] Ritu Tripathi, Sanjay Agrawal, "Critical Analysis of RSA Public Key Cryptosystem", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, ISSN 2277-128X, July 2014.

[18] Raj J. Jaiswal, Ranu Soni, Prasad Mahale, "Reformed RSA algorithm based on Prime Number", International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Information Technology, 2014.

[19] Akansha Tuteja, Amit Shrivastava, "Faster Decryption and More Secure RSA Cryptosystem", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 11, ISSN 2277128X, November 2014.

[20] Amare Anagaw Ayele, Dr. Vuda Sreenivasarao, "A Modified RSA Encryption Technique Based on Multiple public keys", International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 4, ISSN 2320-9798, June 2013.