Assessment of Work Pedestal on RSA in Text Cryptographic System

Aashish Panwar
Dept. of CSE
MEC, Bikaner
panwar.rocks@gmail.com

Dr. Sunita Chaudhary
Dept. of CSE
MEC, Bikaner
er.sunita03@gmail.com

Dr. Amit Sanghi
Dept. of CSE
MEC, Bikaner
dr.amitsanghi@gmail.com

ABSTRACT: Cryptography is a Greek word, crypto signifies 'hidden or covered up' and graphy means 'study'. The conversion of plain text to cipher text is called as encryption and changing the cipher text to plain text is called as decryption. Cryptographic algorithm further divides in symmetric cryptography and asymmetric cryptography. Symmetric cryptography has only one key for both encryption and decryption, this key is called as secret key or private key. Asymmetric cryptography has two keys, one key is used for encryption this key is called public key and other key is used for decryption this key is called as private key.

In this paper, we survey on the customized advance of RSA by using manifold of public keys and prime numbers. This algorithm is providing more secure communication over the network of text files.

Keywords*: - Cryptography, Asymmetric, RSA, Public Key, Symmetric.*

*****

I- INTRODUCTION

In the present time, web is the fundamental need for correspondence amongst people and facilitates for electronic installment, military correspondence and numerous other private or individual interchanges. For this reason privacy and security is major concern in communication. Cryptography is a most commonly used approach to secure the information and data over the channel. Cryptography is a craft of securing the data over the system by changing over the readable text into unreadable text to shield it from unapproved individual. In an distributed network, when data must be send over system, cryptography assumes imperative part for secure correspondence [1,2,3].

Cryptographic algorithm divided in two ways: symmetric key cryptography and asymmetric key cryptography. Symmetric algorithm has one key called private key for both encryption and decryption. Symmetric-key encryption can be actualized in two different ways: stream cipher and block cipher. In Stream cipher one digit of a message is encrypt at a time and Block ciphers take a more than one bit at a time and consider these digits as a single unit. Then encrypt the numerous digits. Asymmetric algorithms utilize two distinctive key, one key called public key is utilized for encryption and other key called private key is utilized for decryption. One of the general public key cryptosystem is the RSA public key cryptosystem [3].

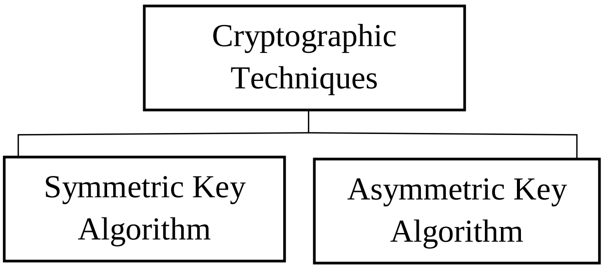

Fig. 1. Types of Cryptography

In this paper we discuss different modified approaches of RSA for secure communication over the network. Modified approaches are more secure and reliable to network. RSA uses two public keys and four prime numbers which are not easily factorable.

1.1 Advantages of Cryptography and RSA based system

1. Secrecy and Privacy

The content of the secret information and communication that is delivered over the network must be only accessible to the authorized sender and the recipient of the information to maintain privacy and security.

2. Integrity

It ensures that the content must not be altered during the exchange phase between sender and receiver over the network; therefore it must stay in its original form to maintain integrity during the whole communication.

3. Authentication

This criterion is very crucial because it ensures that information was send from an authorized sender and received by authorized receiver and decrypt with his private key.

4. Non Repudiation

The sender cannot say that the message was not encrypted with his private/public key because the private/public key used for the encryption is unique.

1.2 Applications of System

1. Secret Communication

By applying cryptography we can send information from one place to another. The modified approach allows us to send secret information's by encrypting it into unreadable form without knowledge of intruders.

2. Encoding the Military Secret Message

The secret information in army or defense services should not be known to enemies or attackers, so to protect such sensitive information our modified approach is quite helpful. The higher authorities of army can send secret information by encrypting it and the authenticated user can decrypt it over other side.

3. Authentication

Authentication is the most common important application of public-key cryptography. By authenticating it ensures us that the data was send by intended sender and also receive by intended receiver.

II- LITERATURE SURVEY

[1] AkanshaTuteja, Amit Shrivastava, invented implementation of a complete RSA encrypt/decrypt method which is based on the study of RSA public key algorithm, in this approach uses 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 transit, 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 secure against low decryption exponentiation attack, because they are using a very large value of d [2].

Limitation - Less secure than existing RSA.

[2] Ritu Tripathi, Sanjay Agrawal, presents survey of RSA algorithm and various modified RSA algorithms. RSA is highly secured algorithm but the drawback of their approach is that it has high computation time and slow speed; so many different techniques are used to enhance the speed of an existing RSA algorithm by applying various modification in original RSA [3].

[3] Amare Anagaw Ayele, Dr. Vuda Sreenivasa rao, proposes a new RSA approach. In that approach they used two public key. These two public keys are sent independently so the hacker cannot get the idea about the keys. The system which required high security but less speed can use this type of approach. The primary thought of this plan is that each conveying party needs only a key pair for communicating with some other imparting party. When somebody acquires a key pair, he/she can speak with any other individual.

Limitation - High security but less speed.

[4] Aayush Chhabra, Srushti Mathur, proposes a new technique which is used for both digital signatures and encryption-decryption. In this approach there is no need to transfer n, this n is the product of two chosen prime numbers, in this way in the public key cryptosystem it becomes difficult for the attacker to decompose n and so the encrypted data stay safe from the hackers [5].

Limitation - Increase in complexity.

[5] Aswathy B.G, Resmi R, presents two architectures implementing modular exponentiation. In the first level two mapping operations are performed parallel with two multipliers. In the second level modular multiplication is done [6].

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

[6] Dr. D.I. George Amalarethinam, J. Sai Geetha, proposed an algorithm in which they achieve an additional level of security. In this approach they used magic rectangle. By utilizing it they build the randomness of the cipher text. In the previous work, when the characters are repeated in the plain text then cipher text is also repeat at that place. It is happened due to ASCII value. In this approach plain text will not repeat again and again. Regardless of whether the redundancy of same character happens, magic rectangle provides different values for every occurrence of that same character. By doing this, it is hard to figure the data being transmitted over system [9].

Limitation – Additional time is required for the making the magic rectangle.

[7] Rajan. S. Jamgekar, Geeta Shantanu Joshi, introduces an approach for transmitting the files securely. There are many places where user needs secure file transmission for example in banking transactions, army related data etc. from the past decades there are many enhancement is done to improve RSA like BATCH RSA, Rebalanced RSA, Multi Prime RSA, R Prime RSA, Multi Power RSA etc. As internet usage is increasing exponentially for e.g. E-mail, chatting, transferring files from sender to receiver and it needs to be secured. This approach centers around document

exchange utilizing modified Secure RSA approach, which disposes of shortcomings of RSA and keep an attacker from taking and abusing information [11].
Limitation -At an instant only one file can be encrypted and transmitted.

[8] Ms. Ritu Patidar, Mrs. Rupali Bhartiya, introduces modified RSA. In this approach it uses the additional third prime number so that modulus n is not easily divisible by intruders. Before the process begins it includes database for storing the key values of RSA cryptosystem. In the introduced method keys are already stored before the process begins. So in compare to traditional RSA method the speed of encryption decryption will increases [12].
Limitation – this approach includes the database which can be easily hacked by hackers.

[9] Li Dongjiang, Wang Yandan, Chen Hong, proposed a method for generation of prime numbers and the public and private keys. Existing method of generating a prime number is very time-consuming, to resolve such problem, an improved algorithm is introduced. As a result, it improves the efficiency of prime number and key generation [13].
Limitation- It is more complex than original RSA.

[10] B. Persis Urbana Ivy, Purshotam Mandiwa, Mukesh Kumar, presents an approach to safe data or information by a modified RSA based on ‘n’ prime. This method presents a new approach which provides very high security for data over the system. In this approach they used ‘n’ prime numbers. Proposed approach is more efficient [14].
Limitation - Complex and time consuming.

[11] Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma, and presents a cryptography algorithm called Modified RSA Encryption Algorithm. Modified RSA is more secured in comparison to existing RSA. The scheme is an additive homo morphic cryptosystem; which means that, if the public-key and the encryption of m1 and m2are given, one can compute the encryption ofm1 + m2 [15].
Limitation - Proposed approach has less speed of encryption, decryption and key generation, takes more time than existing.

[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 increases the speed of 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 Database, and this protocol is responsible for updating the identical gateways database, level selections and establishing the algorithm between gateways [16].
Limitation - It uses database, easily can be attacked by intruders.

[13] Mayank Jhalani, Piyush Singh, Gaurav Shrivastava, they have proposed a new public key cryptosystem. There are various methods which have been introduced to reduce the time for decryption such as Multi Prime RSA etc. They have tried the improvement over Multi Prime RSA to increase the speed of decryption. As compared to Multi Prime RSA, proposed method is much faster and secures [17].
Limitation - Time consuming.

[14] Shilpi Gupta, Jaya Sharma, proposed an approach which is combination of the two algorithms RSA and Diffie-Hellman so that to enhance more security. RSA is a Public key cryptography method. 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 [18].
Limitation - In proposed approach time complexity should be revised for better working of algorithm.

[15] RohitMinni, Kaushal Sultania, Saurabh Mishra, Prof Durai Raj, presents a modified RSA. The new security feature introduced is removing ‘n’ (product of two prime numbers) from the original RSA algorithm. The original RSA algorithm is prone to factorization attacks. The algorithm they presented in this paper is more secure with a slight increase in time complexity [19].
Limitation - In proposed approach time complexity increases.

[16] Xin Zhou, Xiaofei Tang, displays an entire dialog of the cryptography, encryption, decryption, and RSA public key and other related innovation applications in the military, business, protection and different fields of data security which assumes an essential part. Issue for RSA encryption on the document, it shows the RSA mathematical algorithms in the PC businesses significance and its deficiencies. It talks about the inquiries of how to apply to the individual existence of RSA data security issues. At last, they proposed another program to enhance RSA algorithm based on RSA cryptography and the extensive application [20].
Limitation - Complexity increases in proposed approach.

TABLE 1. PREVIOUS WORK BASED ON RSA

S.No.	Authors	Algorithms	Years	Uniqueness
1	Dr. D.I. George Amalarethinam, J.SaiGeetha	Enhancing Security level for Public Key Cryptosystem using MRGA	2015	It uses magic rectangle box for converting character to numerical value.
2	Zhenjiu Xiao, Yongbin Wang, Zhengtao Jiang	Research and Implementation of Four-prime RSA Digital Signature Algorithm	2015	It Intended a four-prime Chinese Remainder Theorem (CRT)-RSA digital signature algorithm.
3	M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya	An Enhanced and Secured RSA Key Generation Scheme	2014	It proposed an approach it which four prime numbers are used instead of two prime numbers.
4	Aswathy B.G, Resmi R	Modified RSA Public Key Algorithm	2014	It presents architecture implementing modular exponentiation
5	Amare AnagawAyele, Dr. VudaSreenivasarao	Modified RSA based on multiple public keys	2013	It proposed an approach which uses two public keys and sent them separately.
6	Ammar Odeh, Khaled Elleithy, MuneerAlshowkan, Eman Abdelfattah	Quantum key distribution	2013	It introduces a quantum algorithm in which public key encryption is employs to generate keys which are improve security over network.
7	NorhidayahMuhammadi, Jasni Mohamad Zaini, MdYazidMohdSaman	i-RSA algorithm	2013	It is proposed that user identity can be used as a public key example is email address. And it can be apply looping process in key generation.
8	Ms. RituPatidar, Mrs. RupaliBhartiya	Modified RSA cryptosystem based on offline storage and prime number.	2013	In order to make modulus ‘n’ large it’s included third prime number and this module is not easily factorable by intruders. To store the key parameters a database system is used.
9	Liang Wang, Yonggui Zhang	Personal information encryption approach based on RSA	2011	It proposed an approach which uses sensitive information such as phone number, address and encrypt it.
10	Malek Jacob Kakish	Enhancing the security of the RSA	2011	It invented a randomized parameter so that even if the same message is send more than one time than still the encrypted message looks different.

[17] Zhenjiu Xiao, Yongbin Wang, Zhengtao Jiang, proposed a modified form of RSA signature algorithm. They try to improve it and more efficient. They proposed a four-prime

Chinese Remainder algorithm in this paper. They used the Hash function SHA512 to make message digest [21].

Limitation – It seems vulnerable to chosen-cipher text attack.

[18] Xianmeng Meng, Xuexin Zheng, they propose short exponent RSA. This approach uses a small parameter *k*. They show that birthday attack may cause this RSA variant insecure. They revisit the birthday attack against short exponent RSA [22].

Limitation - More complex and time consuming.

[19] Dr. Abdulameer K. Hussain, presents a successful method to build the security of conventional RSA algorithm. At the point when the conventional RSA is actualized, there is a circumstance in which the encrypted text (cipher text) is the same as the plain content (original text) at a few values. So it is vital to locate a successful arrangement. With a specific end goal to determine such issue, the proposed strategy acquaint another technique with change the estimation of n by framing an expansive arrangement of prime numbers from which the clients can choose

estimations of it is possible that one prime number or both to guarantee greater security [23].

Limitation - Change in remove over and over to look after security.

III- IMPLEMENTATION

For efficient and effective implementation of any algorithm test data has itself a prime importance. The possibility of algorithm's success is dependent on the test data we have taken. So, we should be very careful about considering the test data. Test data means to make collection of such a data so that complete test of algorithm can be performed that means every condition and every case should be checked through the test data. Keeping in mind the importance of test data everyone should take almost all characters present on the keyboard so that the algorithm can be tested for encryption and decryption of every character.

IV- RESULTS

Security implies keeping data sheltered and secure by hide it from unauthorized get to. So as to keep the information secure has to be protected shielded from unauthorized get to protect during communication. RSA is one of the approaches used to achieve secure communication between two parties in presence of third party called adversaries over the network. Different modified approaches are enhancement form of RSA, which gives more secure way for communication and shorten the time of encryption-decryption and also removes the redundancy problem of cipher text and make the RSA algorithm more secure and aggrandize its usages.

REFERENCES

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

[2] AkanshaTuteja, 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.

[3] RituTripathi, 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.

[4] Amare AnagawAyele, Dr. VudaSreenivasarao, "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.

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

[6] 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**.

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

[8] 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**.

[9] Raj J. Jaiswal, RanuSoni, 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.

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

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

[12] 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**.

[13] 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, ISSN 2319-6378, February 2013.

[14] Ms. Ritu Patidar1, Mrs. RupaliBhartiya, "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**.

[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, 978-0-7695-4789-3/12, 2012,**IEEE**.

[16] B.Persis Urbana Ivy, PurshotamMandiwa, Mukesh Kumar, "A modified RSA cryptosystem based on 'n' prime numbers", International Journal Of Engineering And Computer Science ISSN:2319-7242, Volume1, Issue 2, ISSN 2319-7242, November 2012.

[17] 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**.

[18] Sami A. Nagar, SaadAlshamma, "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**.

[19] Mayank Jhalani, Piyush Singh, Gaurav Shrivastava, "Enhancement over the Variant of Public Key Cryptography (PKC) Algorithm", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 12, ISSN 2250-2459, December 2012

[20] 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**.

[21] 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**.

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

[23] 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.

[24] Robert J Oberg, "Introduction to C# Using .NET", Prentice Hall PTR, ISBN No. 0-13-041801-3, 2002.

[25] Robert Powell, Richards Weeks, "C# and the .NET Framework: The C++ Perspective", Sams publishing, ISBN No. 0-672-32153-x, 2002.