An Improved Cryptosystem based on Shorter Keys and New Security Component using 2k-RSA Algorithm

P Rajak Khan[1], JS Ananda Kumar[2]
[1]*Student, Department of MCA, Kmmips, Tirupati,Andhra Pradesh, India*
[2]*Assistant Professor, Department of MCA, Kmmips,Tirupati,Andhra Pradesh, India*

***Abstract*- Cryptography is used for secure communication since ancient days for providing confidentiality, integrity, and availability of the information. Public key cryptography is a classification of cryptography having a pair of keys for encryption and decryption. Public key cryptography provides security and authentication using several algorithms. RSA algorithm is prominent since its inception and is widely used. Several modified schemes were introduced to increase security in RSA algorithm involving additional complexity. In proposed system, we are used 2k-RSA algorithm. This is same as RSA algorithm but it have extra features. Improve security and these features include dividing the message M by the sender into two parts m1 and m2, and using two keys of shorter sizes (as compared to the original RSA keys), each key is used to encrypt part of the message. In addition to other security information component referred to as Security Card (SeCa). It contains encryption process, keys, and message segments. Mainly components are segment information, size, cipher positin, and keys. By this algorithm improve the performance in terms of increasing security and reducing the computation overhead by decreasing encryption and decryption times.**

***Index Terms*- Cryptography, RSA algorithm, 2k-RSA algorithm, Security Card**

I. INTRODUCTION

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of an integer is hard. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two dissimilar keys i.e. Public Key and Private Key**.** As the name describes that the Public Key is given to everyone and Private key is kept private.

Public-key cryptography is also known as asymmetric-key cryptography, to distinguish it from the symmetric-key cryptography we have studied thus far. Encryption and decryption are carried out using two different keys. The two keys in such a key pair are referred to as the public key and the private key. With public key cryptography, all parties interested in secure communications publish their public keys.

The security of RSA algorithm depends on the ability of the hacker to factorize numbers. New, faster and better methods for factoring numbers are constantly being devised. Obviously the longer a number is the harder is to factor, and so the better the security of RSA. As theory and computers improve, large and large keys will have to be used. The advantage in using extremely long keys is the computational overhead involved in encryption/decryption. This will only become a problem if a new factoring technique emerges that requires keys of such lengths to be used that necessary key length increases much faster than the increasing average speed of computers utilizing the RSA algorithm. RSA's future security relies solely on advances in factoring techniques.

The 1024-bit RSA key is proved to be robust against cryptanalysis attacks due to the difficulty to factorize

it into its basic prime factors. However, as computation power increases and the factorization methods improve, this will change the fact that a 1024-bit key size is really secure, and impose the need to use longer keys (e.g. 2048 bit, 3072 bit or more) to perform encryption.

The main question that arises in this context is: When to make a transition to a longer key size? Moreover, when will using larger key sizes be stopped? In this paper, the researchers investigate the use of multiple shorter keys along with new security component called SeCa to achieve more robustness against cryptanalysis attacks by increasing the workload required by the cryptanalyst to decrypt the ciphertext and get the corresponding plaintext.

II.SECA CONSTRUCTION

The SeCa is a major concept and an essential step of our proposed scheme. It contains details about the encryption process, keys, and message segments. Following are the components of SeCa: Segments Information (SI): contains the original message length (L) and the lengths of the two ciphers (originating from encrypting m1 and m2) and embedded within the encrypted message.

Segments Information Size (SIS): the size of SI. Segments Information Cipher Position (SICP): the position of the SI Cipher (SIC) within the encrypted message, C. Segments Information Key (SIK): the key used to encrypt the (SI).

III.ALGORITHM

2K-RSA ALGORITHM:

Our proposed 2K-RSA algorithm, as the case of RSA, involves three main operations: key generation, encryption, and decryption. When a sender (Alice) intends to communicate a message M with a receiver (Bob), two pairs of keys k1 and k2 are generated. Alice uses Bob's both public keys to encrypt the message, while Bob uses his two private keys as well as the SeCa to decrypt the resulted ciphertext and retrieve the original message M back.

THE ENCRYPTION OPERATION:

At Alice's side, the encryption process is performed as the following: a message M to be communicated is loaded into a 2-dimentional array [r*c], where r is the number of rows and c is the number of columns. Then it is divided into two parts m1 and m2 where the size of each part (mi) is computed as the following:

Size of mi=r/2*c

Alice uses Bob's public keys k1 and k2 to encrypt m1 and m2 to get c1 and c2 , respectively. The size of k1 and k2 is always smaller than the key used in RSA. Finally, the whole ciphertext C is constructed by concatenating c1, c2, and SIC, stored in an array according to the predefined SICP parameter and then sent to Bob.

The extra security of the encryption operation is achieved in particular by the way the whole cipher C is constructed, which depends on the SICP that is determined by the sender in advance and sent to the recipient as part of the SeCa.

The proposed encryption scheme which is called the Two-Key RSA algorithm (2K-RSA). The main procedures of the proposed algorithm are similar to RSA. However, 2K-RSA uses new features to enhances security; these features include dividing the message M by the sender into two parts m1 and m2, and using two keys of shorter sizes (as compared to the original RSA keys), each key is used to encrypt part of the message.

The cryptanalyst needs much extra time and trails to find SI. She does not know its position in the ciphertext nor its size, so the only way left for her is to try encrypting the ciphertext byte by byte, which is clear how much time and trails she needs. Even if she can find and encryp SI, she still needs to restore M from both m1 and m2 in their correct order. This, in turn, increases the effort and time on the cryptanalyst.

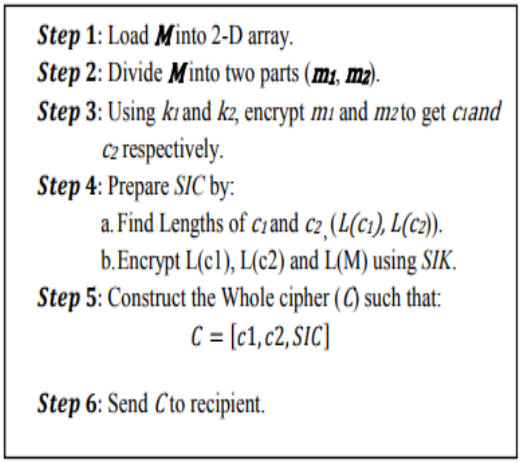

Fig: 2k-RSA Encryption Process

The major contributions of 2K-RSA encryption scheme are:

- The use of a new special secure information component called SeCa.
- The division of the message M into two parts and the use of multiple shorter keys (2 keys), one for each part of M.
- The use of a 2-dimentional array to represent the message M.

THE DECRYPTION OPERATION:

On the recipient side (Bob), since he has the key-pairs and the SeCa, and upon receiving the whole ciphertext C, he first starts retrieving the SI. To do so, he uses the SIP and the SIS that are known a priori, so he can decrypt SI using the SIK. Having the SI decrypted, he can now retrieve L, L(c1) and L(c2) so as to reserve a square array and start decrypting c1 and c2 to get m1 and m2 . Then, he can store m1 and m2 in the array to retrieve M. A step-by-step clarification of the decryption process is described in Fig

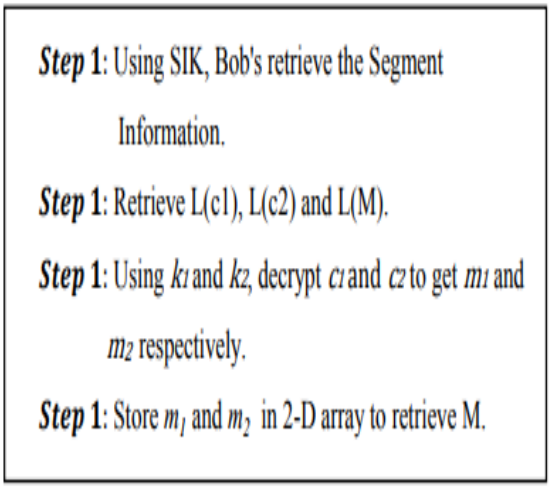

Fig: 2k-RSA Decryption Process

The cryptanalyst needs much extra time and trails to find SI. She does not know its position in the ciphertext nor its size, so the only way left for her is to try decrypting the ciphertext byte by byte, which is clear how much time and trails she needs. Even if she can find and decrypt SI, she still needs to restore M from both m1 and m2 in their correct order.

This, in turn, increases the effort and time on the cryptanalyst. To summarize, the security of the decryption operation relies on the cipher C itself. Since C now is a composite cipher (i.e. contains several sub-ciphers: c1, c2, and SIC) and it results from applying multiple encryption keys, it cannot be decrypted using the traditional methods of attacks that the cryptanalyst uses in RSA. The cryptanalyst needs to find the position of the SIC first which takes her numerous extra steps and trials, after that she still faces the challenge of knowing c1 and c2 to be able to decrypt each cipher and get the whole message M.

IV.CONCLUSION:

In this paper, 2k-RSA aslgorithm is used. It uses two keys to perform the encryption or decryption. For each key of size is less than the key in predictable RSA. In addition to use two keys in this system we are uses security component is SeCa. These components are segment information, size, cipher positin, and keys. By this algorithm improve the performance in terms of increasing security and reducing the computation overhead by decreasing encryption and decryption times.

REFERENCES

[1] Farheen Sultana,Bikiran Choudhury , Shobha M.S ,Dr.Jitendranath Mungara “A Study on Data Encryption Using AES and RSA” 2017.

[2] B.Nithya, Dr.P.Supriya, “A Review of Cryptographic Algorithms in Network Security” 2016.

[3] Srinivas B.L et.al. “A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm” International Journal of Innovative Research in Computer and Communication Engineering, Vol 2, No.5, (2014), pp.77-88.

[4] Swati Kashyap, Er.NeerajMadan “A Review on: Network Security and Cryptographic Algorithm” International Journal of Advanced Research in Computer Science and Engineering, Vol 5, No. 4 (2015), pp.1414-1418.

[5] Rajdeep Bhanot, Rahul Hans “A Review and comparative Analysis of Various Encryption Algorithms” International Journal of Security and its Applications, Vol 9, No. 4, (2015) pp.289-306.

[6] Data Encryption and Decryption Using RSA Algorithm in a Network Environment ,Nentawe

Y. Goshwe. Department of Electrical/Electronics Engineering ,University of Agriculture, Makurdi IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013 .

[7] Chehal Ritika, Singh Kuldeep. "Efficiency andSecurity of Data with Symmetric Encryption Algorithms". International Journal of AdvancedResearch in Computer Science and Software Engineering, ISSN: 2277 128X , Volume 2, Issue 8,August 2012,

[8] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption",in 6 th International Forum on Stratergic Technology(IFOST),2011

[9] Dipali B. Khairnar, Prof. Sandeep Kadam, "Secure RSA: Pair Wise Key Distribution using Modified RSA Algorithm" 2016.

[10] Allam Mousa , "Sensitivity of Changing the RSA Parameters on the Complexity and Performance of the Algorithm", ISSN 1607 – 8926, Journal of Applied Science, Asian Network for Scientific Information, pages 60-63,2005

[11] K. Sheela, E. George Dharma Prakash Raj, "InKeSi- Increased Key Size Method in SRNN Public Key Cryptography Algorithm",IJCSMC, Vol. 2, Issue. 8, August 2013

[12] Sonal Sharma, Jitendra Singh Yadav and Prashant Sharma, "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012, pp 134-138.

[13] Hardik Gandhi , Vinit Gupta ,"A Research on Enhancing Public Key Cryptography by The Use of MRGA with RSA and N-Prime RSA" 2015.

[14] Gopinath Ganapathy, and K.Mani , " Add-On Security Model for public key Cryptosystem Based on Magic Square Implementation", ISBN 978-988- 17012-6-8, Proceedings of the world congress on Engineering and Computer Science 2009 Vol I, San Fransisco, USA.

[15] Sonia Goyat.," Genetic key generation for public key cryptography ",International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[16] Srinivas B.L , Anish Shanbhag , Austin Solomon D'Souza "A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm" 2014