Volume 6, Issue 4, April 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure RSA: Pair Wise Key Distribution using Modified RSA Algorithm

Dipali B. Khairnar, Prof. Sandeep Kadam
Dr.D.Y.Patil College of Engineering, Ambi University of Pune,
Maharashtra, India

Abstract – In this paper we introduced Pairwise key distribution scheme by using modified RSA Algorithm. Main goal of Pairwise RSA Encryption Algorithm is secure transmission of confidential information over network. RSA encryption algorithm is Public key cryptography is also called as asymmetric key cryptography. Public key cryptosystem use keypair one use as public other use as private or secret key and private key cryptosystem use same private key for encryption and decryption.For encryption and decryption RSA encryption algorithm use key pair one key use for encryption which called as public key and other key use for decryption called as private key. In this paper, we have done an efficient implementation of Pairwise RSA algorithm using key pairs and using Euclidean algorithm rather than sending the e value directly as a public key. Because it avoid mathematical attacks and brute force attack. In this paper key size increased 512bit to 1024 bit in Pairwise RSA which provide highest security in the network.

Key terms: Encryption, Decryption, Public key cryptography, Pairwise RSA.

I. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties over network. It is the art of protecting the information by transforming it into plaintext to ciphertext format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text. Cryptography is a technique which use transparency method means hiding the plain information from the web. By using cryptography we can assist this confidential information by secrete writing on our computer network. Cryptography renders the message unintelligible to outsider by various ways of transformations. Data Cryptography is the scrambling of the content of various data forms like text, image, audio and video to make it unreadable or unintelligible during secure file transmission. Its main goal is to keep the data secure from unauthorized access and hackers. In symmetric-key cryptography or private key cryptography, the sender and receiver of a message know and use the same secret key [14]. The main challenge in the network is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phone system, or some other transmission medium to prevent the disclosure of the secret key pair. Anyone who intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key.Because all keys in a secret-key cryptosystem must remain secret, secret-key cryptography often has various difficulty providing secure key management. To solve the private key management problem, Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography or Asymmetric cryptography in 1976. Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret or private and one of which is public. Although different, the two parts of the key pair are mathematically linked with each other.

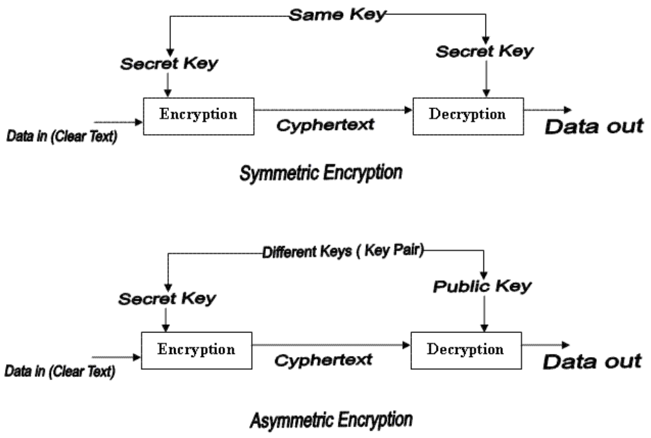


Figure 1: symmetric and Asymmetric Cryptosystem

The algorithms used for asymmetric cryptography are based on mathematical relationships the ones being the integer factorization and discrete logarithm problems [8]. Although it is easy for the recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult for anyone to derive the private key, based only on their knowledge of the public key cryptosystem. Unlike symmetric key algorithms, a public key algorithm does *not* require a secure initial exchange of one or more secret keys between the sender and receiver. In practice, only a hash of the message is typically encrypted for digital signature verification purposes. Public-key cryptography is a fundamental, important, and widely used technology for internet. It is an approach used by many cryptographic algorithms and cryptosystems. Examples of well-regarded asymmetric key techniques for varied purposes include: Diffie–Hellman key exchange protocol, El Gamal, DSS -Digital Signature Standard, which incorporates the Digital Signature Algorithm, Various elliptic curve techniques, Various password-authenticated key agreement techniques, RSA encryption algorithm, Cramer–Shoup cryptosystem, YAK authenticated key agreement protocol, Key exchange methods . Among all RSA is most popular and secure public key cryptographic method [15].
The proposed algorithm is similar with RSA with some modification. Proposed algorithm is also a public key cryptography algorithm. In this algorithm we have extremely short range natural number similar to RSA encryption algorithm [9].

II. LITERATURE SURVEY

1] Modified RSA Encryption Algorithm (MREA):

The algorithms (RSA & MREA) have many important parameters affecting its level of security and speed [10].

By increasing the modulus length it is caused of increasing the complexity of decomposing it into its factors. This also increases the length of private key and hence difficulty to detect the key. Another parameter is modular multiplicative inverse. Where the modular multiplicative inverse is new factor of private key, so it will be more difficult to choose by trying all possible private keys for brute force attack hence the security also increases as well as difficulty of detecting the private key. The RSA and MREA parameters are changed one parameter at a time and the others are kept fixed to study the relative importance [7].

2] File Encryption and Decryption Using Secure RSA:

The algorithms (RSA & MREA) have many important parameters affecting its level of security and speed. By increasing the modulus length it is caused of increasing the complexity of decomposing it into its factors. This also increases the length of private key and hence difficulty to detect the key. Another parameter is modular multiplicative inverse μ where the modular multiplicative inverse μ is new factor of private key, so it will be more difficult to choose μ by trying all possible private keys (brute force attack) hence the security also increases as well as difficulty of detecting the private key. The RSA and MREA parameters are changed one parameter at a time and the others are kept fixed to study the relative importance. The results vary depending on type of file and size of file [11].

3] A Modified RSA Encryption Technique Based on Multiple public keys

RSA Encryption algorithm provide single public key, Less communication overload, More vulnerable to brute force attack, less security, The Public key is sent once. As compare with RSA Modified RSA provide Use two public key, High communication overload, less vulnerable to brute force attack, more security, The Public key is sent separately twice [6].

4] InKeSi-Increased Key Size Method in SRNN Public Key Cryptography Algorithm :

The 1024bit InKeSi SRNN implementation the methodology for computing the modular exponentiation is used. This is chosen because it can achieve an appreciable decrease of covered area and sometimes increase the time-performance comparing with other methodologies.
The senders encrypt the message with Public Key of InKeSi SRNN algorithm and then the data is signed with the Private Key of InKeSi SRNN algorithm. The verification of digital signature is started after this process with the help of Public key at the recipient side. The decryption of the digital signature is done in this process which eventually results in the generation of message [5].

III. IMPLEMENTATION DETAILS

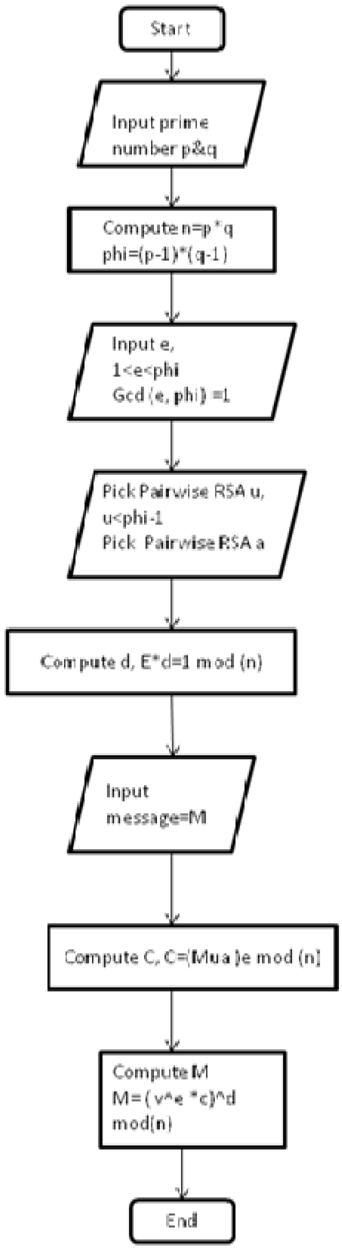
Key Generation by Pairwise RSA Algorithm:

The following flowchart shows the Pairwise RSA algorithm functions**:**

In this module the Pairwise RSA algorithm is used with two random prime numbers of p and q of bit length equal to 1024 bytes. The random number of p and q should not be repeated so we make use of two natural numbers u and a. By using the public key and private key of the sender is created with digital signature [5].

Encryption process

In this the user A makes use of this public and private key creates a digital signature and sends the digital signature with the message to the user B by using the private key of user A[5].


Start
Input prime number p&q
Compute n=p*q phi=(p-1)*(q-1)
Input e, 1<e<phi Gcd (e, phi) =1
Pick Pairwise RSA u, u<phi-1 Pick Pairwise RSA a
Compute d, E*d=1 mod (n)
Input message=M
Compute C, C=(Mua)e mod (n)
Compute M M= (v^e *c)^d mod(n)
End

Decryption Process

User (B) receives Message and Signature. User (B) applies public key to the signature to create a copy of the message and extracts the message. Now user (B) compares the value of Message M with the value of M. If the two values are same, User (B) accepts the message otherwise not [5].

Key generation Process

- Generate two large random prime p, q.
- Compute n=p*q
- Compute phi=(p-1)(q-1)
- Choose an integer e, 1<e<phi, such that gcd (e, phi)=1 compute the such that (e*d) mod phi=1
- Pick short range natural number **u** randomly such that u<phi-1
- Pick another Short range natural number **a** randomly such that phi>a>u And compute ua
- Find d such that e*d mod ((p-1) (q-1)) =1
- Public key is (n, e, ua)
- Private Key is (d, a, u)

  p, q, phi should also be kept secret.

Encryption Process

- Obtains the recipient’s public key (n, e, ua)
- Represent the plaintext message as positive integer M
- Computes the cipher text C=(m ua)e mod n

Send the cipher text C to recipient.

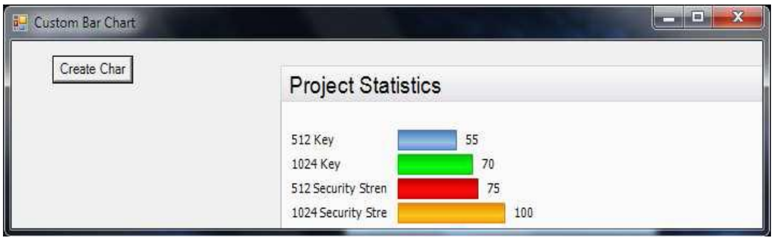
Decryption Process

- Use Recipient private key(d, a , u)
- compute M=(ve c)d mod n where v= uphi-a mod n
- Extracts the plaintext from the integer representative M

Platform: The simulation result of the algorithm Pairwise RSA, implemented in JAVA [12], running on a 2.20 GHz Dual Core Processor and 1 GB RAM has used a 1000 characters long message for encryption/decryption. The algorithms (RSA & Pairwise RSA) have many important parameters affecting its level of security and speed [13]. By increasing the modulus length it is caused of increasing the complexity of decomposing it into its factors. This also increases the length of private key and hence difficulty to detect the key. Another parameter is modular multiplicative inverse. Where the modular multiplicative inverse is new factor of private key, so it will be more difficult to choose by trying all possible private keys (brute force attack) hence the security also increases as well as difficulty of detecting the private key. The RSA and Pairwise RSA parameters are changed one parameter at a time and the others are kept fixed to study the relative importance.

IV. RESULTS

From the implementation of below figure show that the Pairwise RSA algorithm provides 100% Security than the 512bit RSA algorithm.



Pairwise RSA algorithm is similar with RSA with some modification. Pairwise RSA algorithm is also a Public key cryptography algorithm. In this algorithm we have extremely large number that has two prime factors. In addition this we have used two short range natural numbers in pair of keys. One key (public key) for encryption and other corresponding key (private key) for decryption.

.

V. CONCLUSION AND FUTURE SCOPE

RSA algorithm is used to two pair of keys, one for encryption and other corresponding key must be used for decryption. No other key can decrypt the message .RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, *n*, that is the product of two prime numbers. Pairwise RSA algorithm is also a Public key public key cryptography algorithm. Pairwise RSA algorithm is similar with RSA with some modification. Pirwise RSA algorithm is used to encrypt files and transmit encrypted files to other end where it is decrypted for secure file transmission. As a future work multiple file encryption and decryption can be possible with large size files. The project works efficiently for small size while it consumes more time for large size of files. At an instant only single file can be encrypted and transmitted.

ACKNOWLEDGEMENT

Our sincere thanks go to Dr.D.Y Patil College of engineering for providing a strong platform to develop our skill and capabilities. We would like to thanks all those who directly or indirectly help us in presenting the paper. We hereby take this opportunity to express our heartfelt gratitude towards the people whose help is very useful to complete our project work on the topic of "Secure RSA: Pairwise Key distribution Scheme by using modified RSA Algorithm". We would like to express our heartfelt thanks to my guide Prof. Sandeep Kadam whose experienced guidance became very valuable for us.

REFERENCES

[1] William Stallings, *Cryptography and Network Security,Pearson Education*, Fourth Edition.

[2] Xin Zhou, Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption*", IEEE, 6th International Forum on Strategic Technology, pp- 1118 – 1121*

[3] R.L. Rivest, A. Shamir and L. Adleman, "A Method of Obtaining Digital Signatures and Public Key Cryptosystems",*Communication of the ACM, 21, 2(1978),pp 120-126*

[4] Qing LIU, Yunfei LI,Tong LI, Lin HAO "The Research of theBatch RSA Decryption Performance",*Journal of Computational Information Systems 7:3 (2011) 948-955*

[5] 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*

[6] A. 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, June 2013*

[7] Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma,"Modified RSA Encryption Algorithm (MREA)", *2012 Second International Conference on Advanced Computing & Communication Technologies, 978-0-7695-4640-7/12 $26.00 © 2012 IEEE*

[8] Yaun Xue "*Public Key Cryptography and RSA Algorithm"*,Technical notes and papers.

[9] 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.*

[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] Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", *International Journal of Emerging Science and ngineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013*

[12] Neal R. Wagner, "*The Laws of Cryptography with Java Code*", Technical Report, 2003, pages 78-112.

[13] 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.*

[14] Atul Kahate, "*Cryptography and Network Security*", *ISBN-10:0-07-064823-9, Tata McGraw-Hill Publishing Company Limited, India, Second Edition, pages 38-62,152-165,205-240.*

[15] Gagandeep shahi, Charanjit singh "Cryptography and its two Implementation Approaches" *International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 3, May 2013,PP 668-672.*