Survey Paper on Secure File Transmission Using Pairwise RSA Key Generation

Ms.Dipali B. Khairnar
Dr.D.Y.Patil College of Engineering, Ambi
University of Pune, India.

Prof. Yogesh Sayaji
Dr.D.Y.Patil College of Engineering, Ambi
University of Pune, India.

Abstract

Public key cryptography is also known as asymmetric cryptography which refers to a cryptographic algorithm which requires two separate keys at sender and receiver side respectively, one of which is private and other is public. RSA encryption algorithm is public key cryptography to provide security for file transmission over network. RSA might prevent unauthorized access from hacker and misuse of confidential data. Today's world Internet access is increasing for individuals, organizations, and company's .governments exponentially; it is used for connecting peoples through email, chatting, transferring data and files from one end to other. Simple RSA is not perfect for confidential file transmission so we developed improved RSA algorithm as Pairwise RSA. This algorithm solve brute force attack problem. In this paper, Pairwise RSA algorithm 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.

Keywords: Cryptography, Public key, RSA, Asymmetric key, security

1. INTRODUCTION

Cryptography is the Science of using mathematics to encrypt and decrypt information, store sensitive information or transmit it across insecure networks [1]. So that it cannot be read by anyone except the intended recipient, while cryptography is the science of security. Cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Within the context of any application-to-application communication, there are some specific security requirements [5], including:

- *Authentication:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message.

The algorithms used for public key cryptography are based on mathematical relationships (the ones being the integer factorization and discrete logarithm problems).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. This is why, 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 signature verification purposes. Public-key cryptography is a fundamental, important, and widely used technology[1]. 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. Among all RSA is most popular one. 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 large number that has two prime factors similar to RSA) In addition of this we have used two public pair of keys. This modification increases the security of the cryptosystem. So its name is LEE public key algorithm [6].

2. CRYPTOGRAPHY AND TYPES

Cryptography uses the process of transposition and substitution of the characters to hide and retrieve the data. At the sender side we call it Encryption and at the receiver side we called it decryption as shown in figure.1. We use the various keys to encrypt a decrypt the data. Keys are the special digital functions or methods that convert the plain text into inscribe format and it's vice versa. Every element of the network have two keys namely private or personal key which is known to a particular person and public key which is known by all persons in the network. There are two types of cryptography [6].

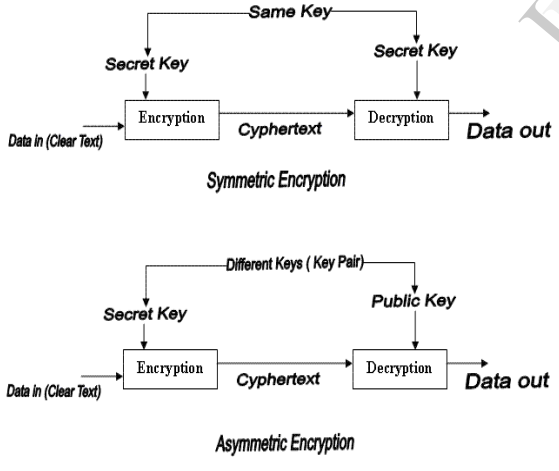

Figure 1.symmetric and Asymmetric Cryptosystem

A] Asymmetric key cryptography or Private Key cryptography:

In this type of cryptography the receiver and sender applies the same key to encrypt and decrypt the message or recover the plaintext from cipher text and vice versa, so this type of cryptography is also known as symmetric encryption and decryption. As shown in figure is showing the whole process of encryption and decryption which is carried out through receiver private key. Through this cryptography form, it is obvious that the secret key must be known to both the sender and the receiver that why it is known as private key cryptography. Transmitting the secret key on insecure network can also destroy the security [6].

B] Different key cryptography or public key cryptography:

In this type of cryptography, the receiver and sender apply the Different keys to encrypt and decrypt the message or recover the plaintext from cipher text and it's vice versa. This type of cryptography is also known as asymmetric encryption and decryption. Figure is showing the whole process where receiver's public key is used for encryption and receiver's private key is used for decryption. In public key cryptography, each user or the workstation take part in the communication have a pair of keys, a public key and a private key and a set of operations associated with the keys to do the cryptographic operations. Only a particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the algorithms, it can be easily exchanged online [6].

3. RSA ENCRYPTION AND DECRYPTION:

RSA is generally used in encrypted connection, digital signatures and digital certificates core algorithms.
Public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA) [3]. It is the main operation of RSA to compute modular exponentiation. Since RSA is based on arithmetic modulo large numbers, it can be slow in constraining environments [4]. Especially, when RSA decrypts the cipher text and generates the signatures, more computation capacity and time will be required. Reducing modulus in modular exponentiation is a technique to speed up the RSA decryption. The security of RSA comes from integer factorization problem. RSA algorithm is relatively easy to understand and implement RSA algorithm is based on the theory of a special kind of reversible arithmetic for modular and exponent RSA is used in security protocols such as IPSEC/IKE, TLS/SSL, PGP, and many more applications. The public and private keys are functions

of a pair of large prime numbers and the necessary activities required to decrypt a message from cipher text to plaintext using a public key is comparable to factoring the product of two prime numbers.

RSA File Transmission Algorithm can be summarized as follows:

1. Generate the asymmetric keys with required digits.

2. Save and load the key, the key is saved as plain text.

3. Use specified key to encrypt any file with RSA algorithm.

4. Encrypted files can be loaded and decrypted with the specified key to restore the original file.

Attacks on RSA

It is important to mention some attacks as follows:
a. Relation to factoring
b. Small Encryption Exponent b
c. Small Decryption Exponent a
d. Forward Search Attack
e. Multiplicative Properties
f. Common modulus attack

g. Message Concealing

h. Cycling attacks

4. KEY GENERATION BY PAIRWISE RSA ALGORITHM

Pairwise RSA for secure file transmission algorithm is divided in to four parts as:

1. Selecting file for transmission
2. Encryption of file
3. Transmission of encrypted file
4. Decryption of file at other end.

In this module Pairwise 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.

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.

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.

Key generation Process[5]:
- 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 u_a
- Find d such that e*d mod ((p-1) (q-1)) =1
- Public key is (n, e, u_a)
- Private Key is (d, a, u)

P, q, phi should also be kept secret.

Encryption Process[5]
- Obtains the recipient's public key (n, e, u_a)
- Represent the plaintext message as positive integer M
- Computes the cipher text C=(m u_a)$_e$ mod n

Send the cipher text C to recipient.

Decryption Process[5]
- Use Recipient private key(d, a , u)
- compute M=(v_e c)$_d$ mod n where v= u_{phi-a} mod n
- Extracts the plaintext from the integer representative M

Advantages of Pairwise RSA algorithm [5]:
- The primary advantage of public key cryptography is increased security.
- It provides digital signature that cannot be repudiated.
- We can select large prime numbers for enhancement of security of keys.
- Public key cryptography may be used with secret key cryptography.

Three approaches to attacking Pairwise RSA[5]:
- Brute force attack (size of numbers)
- Mathematical attack (modulus N)
- Timing attack (running of decryption)

5. Conclusion

In this paper an algorithm is designed for RSA a method for implementing a public-key cryptosystem

using two public key and some mathematical relation. Pairwise algorithm is similar with RSA with some modification. Pairwise 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. This modification increases the security of the cryptosystem. So its name is short range natural number public key algorithm.

6. References

[1] William Stallings, Cryptography and Network Security, Pearson Education, Third 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]"The Research of the Batch RSA Decryption Performance", Qing LIU, Yunfei LI,Tong LI, Lin HAO,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]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, June 2013