TOJSR
The Oxford Journal of Science and Research

ISSN No.: 2581-9380
TOJSR, 2019, 2 (1), 1-3

An in Depth Study of the Rivest Shamir Adleman Public Key Cryptography

Sajana Balan Manian*

Department of Computer Science and Applications, The Oxford College of Science, Bengaluru, India

KEYWORDS: *Public key cryptography, private keys, public keys,RSA, encryption, decryption, security*

ABSTRACT: Security is an important concept in the day to day life. No matter whatever we do, there are several aspects of security to be dealt with. When we go for online transactions or chatting etc the security of the information is a very important matter. From the olden times there have been various methods of providing security for our information. But with the intent of time all the classical methods of security are not reliable because it is prone to attacks. Hence the concept of public key cryptography has been evolved and the Rivest Shamir Adlemann algorithm is one such technique.It isnecessary to see that the information is known only to the sender and the receiver. The aim of this paper is to study in detail the working of RSA (Rivest Shamir Adlemann) algorithm with the help of example.

INTRODUCTION

Cryptography has been derived from two Greek words "*kryptos*" meaning secret and"*graphia*" meaning writing. Hence cryptography is called the art of secret writing. There are two methods of cryptography

(a) *Conventional Cryptography:* - It is the oldest method of cryptography in which the same key is used for both encryption and decryption. It is not asecure method of cryptography because of the usage of a single key and it is prone to attack.

(b) *Public key Cryptography*: - It is the method of cryptography in which two different keys are used for encryption anddecryption. It is a secure method of cryptography as the keys are not shared.

Conventional Cryptography

The following are a part and parcel of any cryptographic technique

(a) Plain Text: - The original message which has to be send.Example: - hello

(b) Cipher Text: - The converted form of the plain text Example:-ifmmp

(c) Key: - It is the secret information needed to convert a plain text to a cipher text and vice versa. Example: - Here we can see that each element of the plain text has been converted to the next element in the English Alphabet. Hence the key is +1 for encryption and -1 for decryption

(d) Encryption Algorithm: - It is a set of mathematical operations which take plain text and key as the input to produce the cipher text.

(e) Decryption Algorithm: - It is a set of mathematical operations which take cipher text and key as the input to produce the plain text.

But in this method we can see that if the key is compromised, then it is possible for an attacker to gain access to information.

Public key Cryptography

In order to prevent this public key cryptography has been developed. All the above contents are the same except for the key. Instead of a single keythere will a pair of keys called the public key, private key pair.

The public key is represented using *KU* whereas the private key is represented as *KR*. The public key will be known to everyone involved in the data transfer because of which

*sajanabalan@gmail.com

ISSN No.: 2581-9380
TOJSR, 2019, 2 (1), 1-3

it is used for encryption by the sender, whereas the private key will be known only to the generator of it. Hence it is used for decryption. The most important concept is that the public key and private key should always be chosen in a pair, failing which the receiver will not get the correct plain text.

METHOD

In this paper an indepthstudy of the (Rivest Shamir Adleman) RSA cryptographic technique is performed

RSA Cryptography

The RSA cryptography falls under the category of public key cryptography. So as discussedearlier each user involved in cryptography has to generate their public key private key pair. The public key should be made visible to perform encryption by the sender.

The RSA derives its names from the first letters of the second names of the founders: Ron Rivest, Adi Shamir, and LenAdleman.

There are primarily four steps involved in RSA cryptography.

(a) Key Generation
(b) Key Distribution
(c)Encryption
(d) Decryption

Key Generation:

It indicates the mathematical operations required to generate the public and the private keys for any user.

1. Select two prime numbers p and q such that p and q are not equal.
2. Calculate $n= p*q$ (1)
3. Calculate the Euler's totient using the values from equation (1)
   $\varphi(n)= (p-1)(q-1)$ (2)
4. Select an integer e such that
   $gcd(\varphi(n), e)=1, 1<e<\varphi(n)$ (3)
   obtain the value of $\varphi(n)$ from equation (2)
5. Calculate d such that
   $d=e^{-1}(mod\varphi(n))$ (4)
   Obtain the values of e and $\varphi(n)$ from equation (2) and (3)
6. Public key =(e,n) (5)
   Obtain the values of e and n from equations (3) and (1)
7. Private key =d (6)
   Obtain the values of d from equations (4).

Key Distribution

The user should make the public key available to the others whereas the private key should be kept with the user without disclosing. Public Key = (e, n) can be used by the users to encrypt any information before sending and the PrivateKey =d should be kept a secret.

Encryption

It will be performed by the sender using the public key of the receiver

1. The sender generates a plain text P.
2. The sender calculates the cipher text C
   $C= P^e \bmod n$ (7)

The C will be send to the receiver and it should be decrypted to get the actual plain text.

Decryption

It will be performedP by the receiver using the private key of the receiver.

1. $P=C^d \bmod n$ (8)

The plain text send by the sender should match with the plain text which the receiver has decrypted, in order to be sure that there is no attack. Any change in the plain text value indicates a breach of security.

Example to solve RSA Cryptography

Calculate the public key, private key and the cipher text if n=33 and the plain text is 6.

Step 1 :- **Key Generation:**

(a) n=33.

33 can be converted as aproduct of two prime numbers 3 and 11.

(b) Let p=3 and q=11

(c) $\varphi(n)= (p-1)(q-1)$

$\varphi(n)= (3-1)(11-1)=20$

(d) Let the integer e be the first number which satisfies$gcd(\varphi(n), e) =1, 1<e<\varphi(n)$

Hence let e be 3

(e)$d=e^{-1} (mod\ \varphi(n))$.

d will be the multiplicativeinverse of e

$d= 3^{-1} (mod\ 20) =7$

(e) Public Key =(e, n) = (3, 33)

(f)Private Key = d=7

Step 2:-**Key Distribution**

The generator of the keys of the previous step will send the public key to the user who wishes to send him a secret message.

Step 3:- **Encryption**

It will be performed by the sender using the public key of the receiver.

The plain text is 6

Hence the cipher text will be

$C = P^e \bmod n = 6^3 \bmod 33 = 18$

Step 4:- **Decryption**

It will be performed by the receiver using the private key of the receiver.

The receiver gets the cipher text C=18 from the sender. -

$P = C^d \bmod n = 18^7 \bmod 33 = 6.$

The plain text generated by the sender matches with the plain text generated by the receiver. Hence there is no security breach.

RESULTS ANDDISCUSSIONS

Analysis of the RSA Algorithm

As two different keys are used for encryption and decryption the chances for attack are less. The algorithm is very complex making it impossible for an attacker to easily find out the other key pair. A user can have more than one key pair which he can use for a variety of data transfers and for different users. It is necessary to see that the same key pair is used for encryption and decryption.

CONCLUSION

Hence it is clear that with an efficient public key techniquesuch as RSA algorithm, it is possible to protect the information from getting attacked by others. As shown in the example, RSA can be used to send lots of information securely so that the information is known only to the sender and the receiver.

ABBREVIATIONS

RSA Algorithm – Rivest Shamir Adleman Algorithm, SHA 1- Secure Hash Algorithm DSS- Digital Signature Standard

REFERENCES

1.Behrouz ,Forouzan, Debdeep Mukhopadhyay ,*Cryptography and Network Security.* (2nd edition, Tata McGraw-Hill, 2011).

2.Saranya ,Vinothini, Vasumathi.*A study on RSA Algorithm for Cryptography* .**5**, 5708-5709(2014).

3.William Stallings *Network Security Essentials Applications and Standards*(4th edition, Person Education, 2012).

4. Shivendra Singh, Md Sarfaraz Iqbal, Arunima Jaiswal ,*Survey on techniques developed Using Digital Signature : Public Key Cryptography*.**117**(2015)

5.William Stallings*Cryptography and Network Security*(4th edition, Pearson Education 2012)