*Available online at www.elixirpublishers.com (Elixir International Journal)*

**Computer Science and Engineering**

*Elixir Comp. Sci. & Engg. 87 (2015) 35896-35898*

Elixir
ISSN: 2229-712X

# A modified RSA cryptosystem based on 'N' prime numbers

B.Persis Urbana Ivy, Purshotam Mandiwal and Mukesh Kumar
VIT University Vellore.

**ARTICLE INFO**

**Article history:**
Received: 17 October 2012;
Received in revised form:
15 October 2015;
Accepted: 21 October 2015;

**Keywords**
'n' prime numbers,
Encryption,
Decryption,
RSA Cryptosystem.

## ABSTRACT

To secure data or information by a modified RSA cryptosystem based on 'n' prime. This is a new technique to provide maximum security for data over the network. It is involved encryption, decryption, and key generation. Prime number used in a modified RSA cryptosystem to provide security over the networks. In this technique we used 'n' prime number which is not easily breakable. 'n' prime numbers are not easily decompose. This technique provides more efficiency and reliability over the networks. In this paper we are used a modified RSA cryptosystem algorithm to handle 'n' prime numbers and provides security.

## Introduction

Rivest, Adi Shamir and Leonard Adleman are the developer of the RSA cryptosystem of MIT in 1997.it was described in 1978. Some of the famous security system which is composed of three faces: such as prime Key generation, Encryption and Decryption phase. In this technique we used RSA cryptosystem algorithm. In which included the private key and public key. The public key only used for encrypt the messages and it can be seen to all. It is not secret key. The private key is used for decrypt the messages. Private Key is also called the secret key. In this technique we used 'n' prime number which is not easily breakable. 'n' prime numbers are not easily decompose. This technique provides more efficiency and reliability over the networks. In this paper we are used a modified RSA cryptosystem algorithm to handle 'n' prime numbers and provides security. In which two techniques are used like encryption and decryption. The encryption technique which is used to convert original (plain text) data to cipher text. The plain text is also called the clear text. The plain text is easily read by anyone. Second technique is decryption which is used to convert cipher text to plaintext (readable format).cipher text is also called the unreadable form.

## Literature review:

R.Rivest, A.Shamir and L.Adleman-: A methodology for digital signatures and RSA cryptosystems. In this research paper which is used RSA cryptosystem for digital signature [8]. It is also increased the efficiency and security.

Ravi shanka dhakar - security of RSA cryptosystem depend on the large prime numbers because it is difficult to break the large prime numbers.RSA algorithm provides the security and performance. Every element of the set is greater than all integer numbers [1].In this paper a RSA algorithm which is provided security against brute force attacks.

Hu Zhihu- in this research paper which is used a large prime number RSA cryptosystem for security [2].

The large prime number is not easily factorized. Apparently in this research paper the RSA algorithm is developed for produce the large prime numbers. In which used two large prime numbers.

## Problem definition:

The large number is easily factorized or decomposes and the limited prime numbers are easily decomposed which will not be provided security throw the networks. That's why we used 'n' prime numbers to provide more security throw the networks and it is also not easily factorized.

## Solution Methodology:

In this paper we developed an algorithm that is based on modified RSA cryptosystem based on 'n' prime numbers. This algorithm is useful to getting the high security. We endeavored to evolve 'n' prime numbers for security throws the networks. Because 'n' prime numbers are not easily decomposed and increased the efficiency throw the networks. In the paper we will be used JAVA language to get the private key and public Key.

## RSA algorithm:

- Select two different prime numbers p and q

For security aim, the integer's p and q must be prime numbers.

- Calculate n=p*q

n will be used as the module for public key and private key.

- Calculate f(n)=(q-1)(p-1),

Where f is a function of Euler's

- Select an integer e such that 1<e<f(n) and GCD (e, f(n))=1;

e and f(n) are co prime.

- **Determine d:**

d is multiplicative inverse of e mod (f(n))
(e * d) mod f (n) = 1
d is the private key

## Encryption:

A transfer the data m with the public key (e, n) to B receives the data m with the private key (d, n)
Such that 0<m<n
C=m$^e$ mod n
A will be used the public key and transfer the data plain text to cipher text.

**Tele:**
**E-mail addresses: Prssivy454@gmail.com**

**Decryption:**

B will be gotten the data or message m throws the cipher text to plain text. B is used private key d.

m= $c^d$ mod n

B can recover the original data or message.

**Example:**

Below is given an example of RSA algorithm

In which we will be used four prime numbers and get public key and private key.

Select four prime numbers.

P=2, q=3, r=5, s=17

- Calculate n=p*q*r*s

n=2*3*5*17

- Calculate f(n)=(p-1)(q-1)(r-1)(s-1)

f(510) = (2-1) (3-1) (5-1)(17-1) =128

f (n)=128

- Select any number 1<e<128

F (n) must not be divisible by e

Let e=3

- Select d, multiplicative of e(mod f(n))

d= 43

the public key is(n = 510,e = 3)

private key is (n = 510,d = 43)

Given message m = 11.

Encryption:

C= $11^3$ mod 510 = 311

C = 311

**Decryption:**

M = $311^{43}$ mod 510 = 11

B got the original message (11) which is sent by A.

**Conclusion:**

In this paper we used ‘n’ prime numbers which is provided the security over the networks. In which we endeavored to get the quality that make easier the cryptography to have a good use of ‘n’ prime numbers. The ‘n’ prime numbers act (play) very necessary role in RSA cryptosystem. To develop the RSA algorithm for ‘n’ prime numbers and also used four prime numbers.

**Problem definition:**

The large number is easily factorized or decomposes and the limited prime numbers are easily decomposed which will not be provided security throw the networks. That’s why we used ‘n’ prime numbers to provide more security throw the networks and it is also not easily factorized.

**Solution Methodology:**

In this paper we developed an algorithm that is based on modified RSA cryptosystem based on ‘n’ prime numbers. This algorithm is useful to getting the high security. We endeavored to evolve ‘n’ prime numbers for security throws the networks. Because ‘n’ prime numbers are not easily decomposed and increased the efficiency throw the networks. In the paper we will be used JAVA language to get the private key and public Key.

RSA algorithm:

- Select two different prime numbers p and q

For security aim, the integer’s p and q must be prime numbers.

- Calculate n=p*q

n will be used as the module for public key and private key.

- Calculate f(n)=(q-1)(p-1),

Where f is a function of Euler’s

- Select an integer e such that 1<e<f(n) and GCD (e, f(n))=1;

e and f(n) are co prime.

- Determine d:

d is multiplicative inverse of e mod (f(n))

(e * d) mod f (n) = 1

d is the private key

**Encryption:**

transfer the data m with the public key (e, n) to B receives the data m with the private key (d, n)

*Such that 0<m<n*

C=$m^e$ mod n

will be used the public key and transfer the data plain text to cipher text.

Decryption:

B will be gotten the data or message m throws the cipher text to plain text. B is used private key d.

m= $c^d$ mod n

B can recover the original data or message.

Example:

Below is given an example of RSA algorithm

In which we will be used four prime numbers and get public key and private key.

Select four prime numbers.

P=2, q=3, r=5, s=17

- Calculate n=p*q*r*s

n=2*3*5*17

- Calculate f(n)=(p-1)(q-1)(r-1)(s-1)

f(510) = (2-1) (3-1) (5-1)(17-1) =128

f (n)=128

- Select any number 1<e<128

F (n) must not be divisible by e

Let e=3

- Select d, multiplicative of e(mod f(n))

d= 43

the public key is(n = 510,e = 3)

private key is (n = 510,d = 43)

Given message m = 11.

Encryption:

C= $11^3$ mod 510 = 311

C = 311

**Decryption:**

M = $311^{43}$ mod 510 = 11

B got the original message (11) which is sent by A.

**Conclusion:**

In this paper we used ‘n’ prime numbers which is provided the security over the networks. In which we endeavored to get the quality that make easier the cryptography to have a good use of ‘n’ prime numbers. The ‘n’ prime numbers act (play) very necessary role in RSA cryptosystem. To develop the RSA algorithm for ‘n’ prime numbers and also used four prime numbers.

**References:**

1. RSA algorithm using modified subset sum cryptosystem, Sonal Sharma, Computer and Communication Technology (ICCCT), pp-457-461, IEEE 2011.
2. The large prime numbers based on genetic algorithm, hang Qing, (ICISIE) pp-434-437, IEEE 2011.
3. An advanced secure (t, n) threshold proxy signature scheme based on RSA cryptosystem for known signers, Kumar, R, Dept. of Compute. Sci. and Eng, pp 293-298, IEEE 2010.
4. An efficient decryption method for RSA cryptosystem, Ren-Junn Hwang, Dept. of Compute. Sci. and Inf. Eng, pp-585-590, IEEE 2005.

5. A new RSA cryptosystem hardware design based on Montgomery’s algorithm, Ching Chao Yang, Dept. of Electron. Eng, pp- 908-913, IEEE 1998.
6. A systolic RSA public key cryptosystem, Po – Song Chen, Dept. of Electron. Eng, pp 408-411, IEEE 1996.
7. Blocking method for RSA cryptosystem without expanding cipher length, NEC Corp, Kanagawa, Japan, pp 773-774, IEEE 1989.
8. A method for obtaining digital signatures and public key cryptosystems, R.Rivest, A.Shamir and L.Adleman “communication of the association for computing machinery “ 1978, pp 120-126.
9. http://mathworld.wolfram.com/RSAEncryption.html
10. http://www.mathaware.org/mam/06/Kaliski.pdf
11. http://en.wikipedia.org/wiki/RSA
12. http://www.rsa.com/rsalabs/node.asp?id=2214
13. Cryptography and network security, William Stallings
14. RSA security’s official guide to cryptography, Steve Burnett