Name : Ansari M.Saeem M.Saleem

Uid : 2019430001

Subject : NAD

Expt no : 6

Aim : Write a program for providing security for transfer of data in the network. (RSA Algorithm)

Aim:

Write a program for providing security for transfer of data in the network. (RSA Algorithm)

Objectives:

- To encrypt and decrypt plain text using RSA algorithm in order to provides secure communication over the network.
- To ensures the information are confidential and authenticated.

Theory:

- Under RSA encryption, messages are encrypted with a key called a public key, which can be shared openly. Due to some distinct mathematical properties of the RSA algorithm, once a message has been encrypted with the public key, it can only be decrypted by another key, known as the private key. Each RSA user has a key pair consisting of their public and private keys. As the name suggests, the private key must be kept secret.
- RSA encryption is often used in combination with other encryption schemes, or for digital signatures which can prove the authenticity and integrity of a message.
- Security provided by RSA is based on the difficulty in factoring very large numbers. Based on this principle, the RSA encryption uses prime factorization as the trapdoor for encryption

Methodology :

Algorithm for RSA :

- Key Generation Process :
  - Chose two prime no p and q.
  - Compute the value of n and t (totient function):

    $n = p*q$

    $t = (p-1) * (q-1)$
  - Select a number e that is co-prime with t

    $gcd(e,t) = 1$
  - Compute d such that

    $d * e = 1 \bmod t$
  - Public key is (e,n)
  - Private Key is (d,n)
- Encryption Process :
  - Plain Text = M
  - Cipher Text = C =M^e mod n = 43
- Decryption Process :
  - Decipher Text = M = C^d mod n = 10

Example :

M = 10

p = 11

q = 29

n = p*q

n = 319

t = (p-1) * (q-1)

t = 280

e = 3

d * e = 1 mod n

d = 187

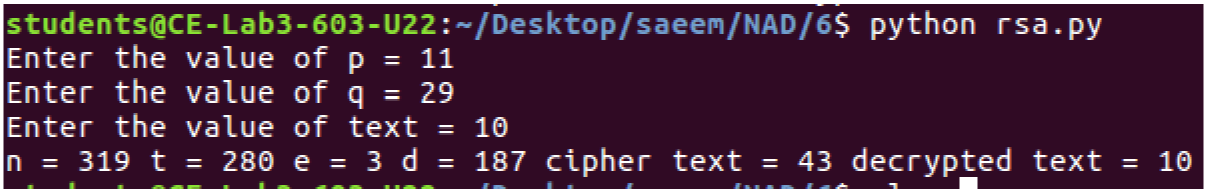
Public Key = (e , n) = (3,319)

Private Key (d , n) = (187 ,319)

C = M^e mod n = 43

M = C^d mod n = 10

Results :



```
students@CE-Lab3-603-U22:~/Desktop/saeem/NAD/6$ python rsa.py
Enter the value of p = 11
Enter the value of q = 29
Enter the value of text = 10
n = 319 t = 280 e = 3 d = 187 cipher text = 43 decrypted text = 10
```

Conclusion:

Here we can conclude that RSA algorithm can be used to encrypt and decrypt plain text in order to provide secure communication in the network.