

| | | |
|---|---------------------------------|-------------------|
| Name of Student: Pushkar Sane | | |
| Roll Number: 45 | Lab Assignment Number: 2 | |
| Title of Lab Assignment: Implementation of Asymmetric key algorithm (RSA). | | |
| DOP: 06-08-2024 | DOS: 13-08-2024 | |
| CO Mapped: | PO Mapped: | Signature: |

Practical No. 2

Aim: Implementation of Asymmetric key algorithm (RSA)

Theory:

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes, the Public Key is given to everyone and the Private key is kept private.

An example of asymmetric cryptography:

1. A client (for example browser) sends its public key to the server and requests some data.
2. The server encrypts the data using the client's public key and sends the encrypted data.
3. The client receives this data and decrypts it.

Advantages:

1. Security: RSA algorithm is considered to be very secure and is widely used for secure data transmission.
2. Public-key cryptography: RSA algorithm is a public-key cryptography algorithm, which means that it uses two different keys for encryption and decryption. The public key is used to encrypt the data, while the private key is used to decrypt the data.
3. Key exchange: RSA algorithm can be used for secure key exchange, which means that two parties can exchange a secret key without actually sending the key over the network.
4. Digital signatures: RSA algorithm can be used for digital signatures, which means that a sender can sign a message using their private key, and the receiver can verify the signature using the sender's public key.
5. Speed: The RSA technique is suited for usage in real-time applications since it is quite quick and effective.
6. Widely used: Online banking, e-commerce, and secure communications are just a few fields and applications where the RSA algorithm is extensively developed.

Disadvantages:

1. Slow processing speed: RSA algorithm is slower than other encryption algorithms, especially when dealing with large amounts of data.

2. Large key size: RSA algorithm requires large key sizes to be secure, which means that it requires more computational resources and storage space.
3. Vulnerability to side-channel attacks: RSA algorithm is vulnerable to side-channel attacks, which means an attacker can use information leaked through side channels such as power consumption, electromagnetic radiation, and timing analysis to extract the private key.
4. Limited use in some applications: RSA algorithm is not suitable for some applications, such as those that require constant encryption and decryption of large amounts of data, due to its slow processing speed.
5. Complexity: The RSA algorithm is a sophisticated mathematical technique that some individuals may find challenging to comprehend and use.
6. Key Management: The secure administration of the private key is necessary for the RSA algorithm, although in some cases this can be difficult.
7. Vulnerability to Quantum Computing: Quantum computers have the ability to attack the RSA algorithm, potentially decrypting the data.

Code:

#Implementation of RSA Algorithm

import math

def gcd(a, h):

temp = 0

while(1):

temp = a % h

if (temp == 0):

return h

a = h

h = temp

p = 3

q = 7

n = p*q

e = 2

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

while (e < phi):

if(gcd(e, phi) == 1):

break

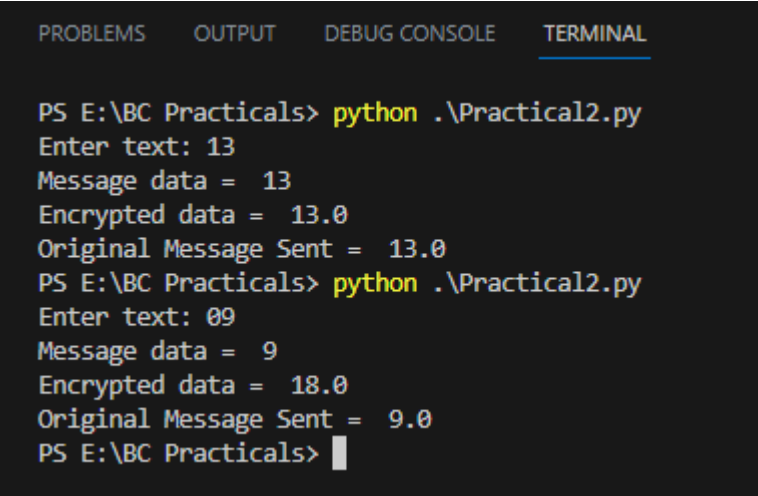
```
        else:
            e = e+1

k = 2
d = (1 + (k*phi))/e

msg = int(input("Enter text: "))
print("Message data = ", msg)

c = pow(msg, e)
c = math.fmod(c, n)
print("Encrypted data = ", c)

m = pow(c, d)
m = math.fmod(m, n)
print("Original Message Sent = ", m)
```

Output:

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL

PS E:\BC Practicals> python .\Practical2.py
Enter text: 13
Message data = 13
Encrypted data = 13.0
Original Message Sent = 13.0
PS E:\BC Practicals> python .\Practical2.py
Enter text: 09
Message data = 9
Encrypted data = 18.0
Original Message Sent = 9.0
PS E:\BC Practicals> 
```

Conclusion:

Successfully demonstrated the implementation of Asymmetric key algorithm (RSA).