Practical No.6

AIM :- To implement an RSA algorithm.

SOFTWARE REQUIRED:-

Operating System: - Ubuntu Python 3

THEORY:-

Introduction to RSA:-

RSA abbreviation is Rivest–Shamir–Adleman. This algorithm is used by many companies to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm which means that there are two different keys i.e., the public key and the private key. This is also known as publickey cryptography because one of the keys can be given to anyone.

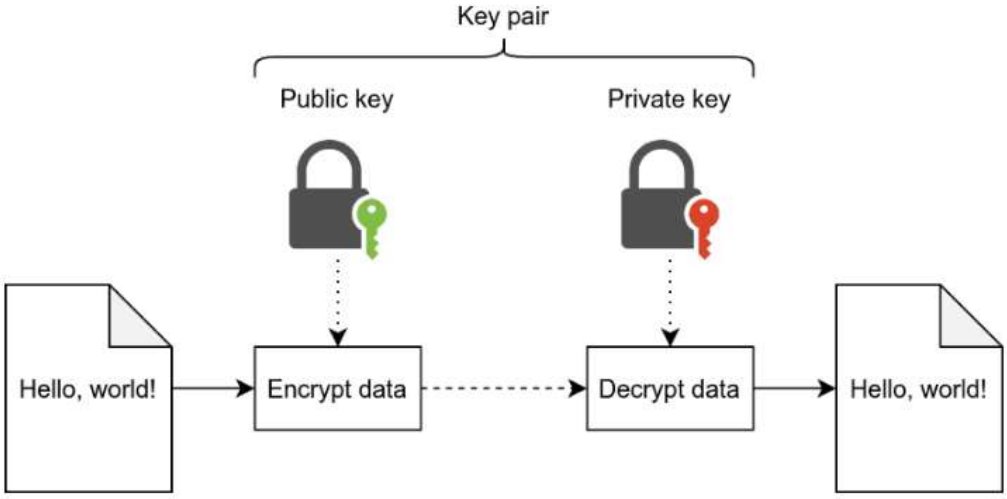
Public key encryption algorithm: Public Key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned a pair of keys:

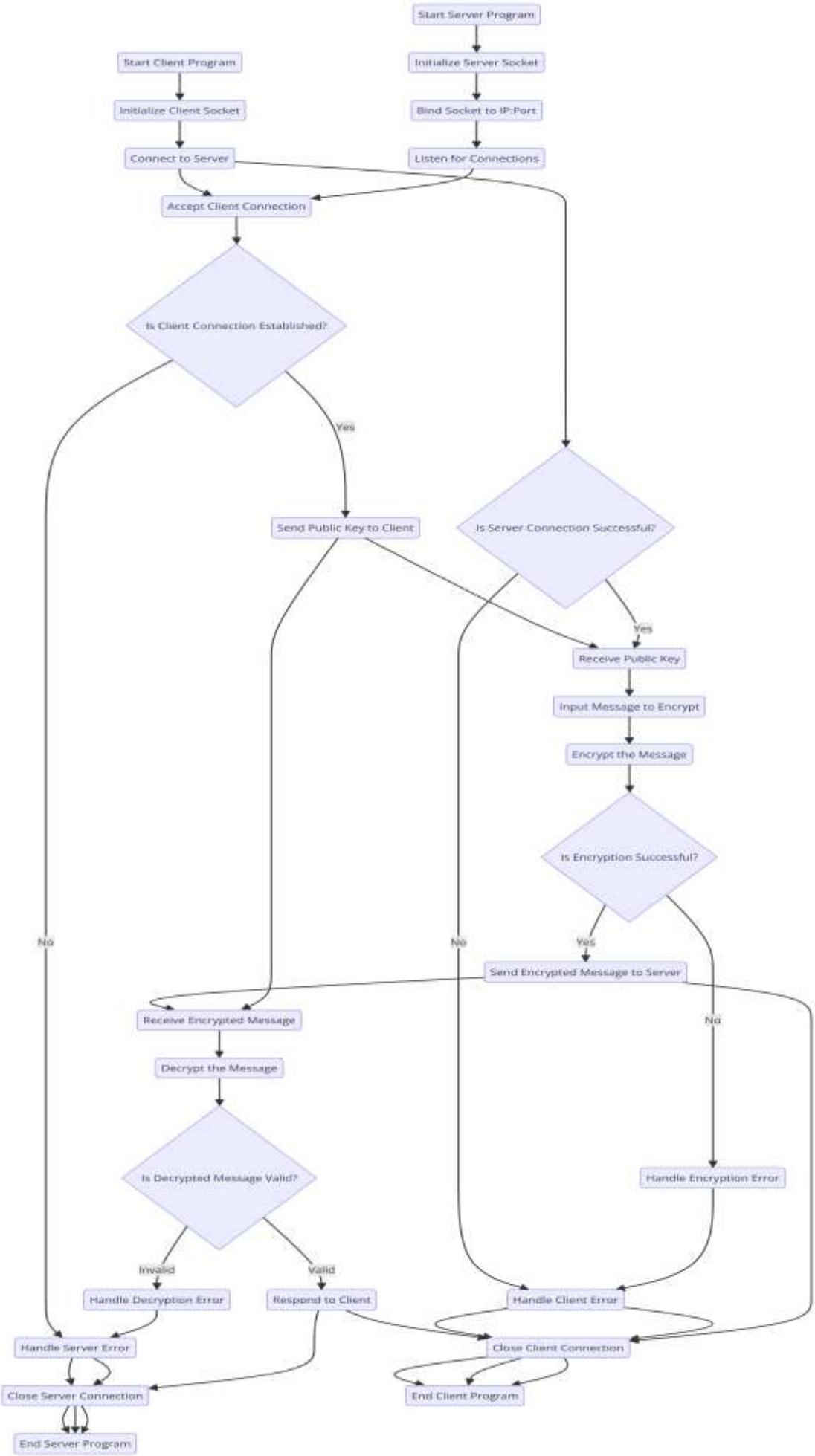
1) Public key
2) Private key

The Public key is used for encryption, and the Private Key is used for decryption. Decryption cannot be done using a public key. The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only to the user who owns the key. It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his private key.

The Public key algorithm operates in the following manner:

1) The data to be sent is encrypted by sender A using the public key of the intended receiver
2) B decrypts the received ciphertext using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
3) A decrypts the received ciphertext using its private key, which is known only to him.




Start Server Program
Initialize Server Socket
Bind Socket to IP:Port
Listen for Connections
Start Client Program
Initialize Client Socket
Connect to Server
Accept Client Connection
Is Client Connection Established?
Yes
No
Send Public Key to Client
Is Server Connection Successful?
Yes
No
Receive Public Key
Input Message to Encrypt
Encrypt the Message
Is Encryption Successful?
Yes
No
Send Encrypted Message to Server
Receive Encrypted Message
Decrypt the Message
Is Decrypted Message Valid?
Invalid
Valid
Handle Decryption Error
Respond to Client
Handle Encryption Error
Handle Client Error
Handle Server Error
Close Client Connection
Close Server Connection
End Client Program
End Server Program

Conclusion:

Thus the program for implementation of RSA algorithm is completed & output is verified.

Course Teacher
Ms. Prajakta Sawle