ASSIGNMENT NO.5

* Aim

Implement a client and a server on different computers using Python. Perform the communication between these two entities by using RSA cryptosystem.

* Theory

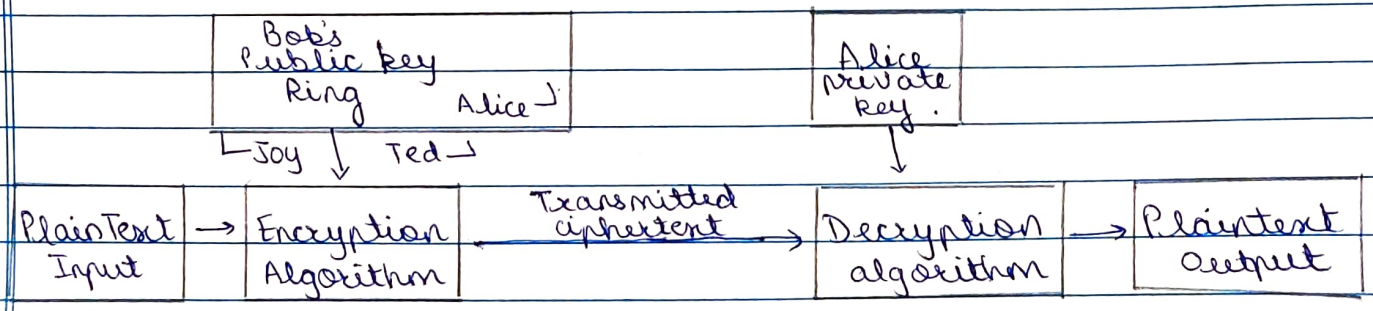
Asymmetric / Public Key Algorithm

This type of algorithm rely on one key for encryption and a different but related key for decryption. These algorithms have following important characteristic

- It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and encryption key.
- Either of two related keys can be used for encryption, with other one used for decryption.

Public key encryption scheme has six ingredients

1) Plaintext : Readable message or data that is fed into algorithm as input.
2) Encryption algorithm : performs transformations on plaintext
3) Public & Private keys : Used for encryption and decryption
4) Ciphertext : Scrambled message produced as output



Decryption Algorithm:

1) Each user generates a pair of keys to be used for encryption and decryption messages.
2) Each user places one of the two keys in public register or other accessible file. This is public key. The companion key is kept private. Each user maintains a collection.
3) If B wishes to send a confidential message to A, B encrypts the message using A's public key.
4) When A receives message, she decrypts it using her private key.

RSA Algorithm

This algorithm includes three steps key generation, encryption and decryption. This scheme is a block cipher in which the plain text and ciphertext are integers between 0 and n-1. Plaintext is encrypted in blocks, having a binary value less than 'n'. Both sender and receiver must know the value of n.

Algorithm:

I 1) Key generation
2) Select p, q p and q both prime, p ! q
3) Calculate $n = p * q$
4) Calculate $\phi(n) = (p-1)(q-1)$
5) Select integer e, such that $\gcd(\phi(n), e) = 1 ; 1 < e < \phi(n)$
6) Calculate $d = e^{-1} \bmod \phi(n)$
7) Public Key $PU = \{e, n\}$
8) Private key $PR = \{d, n\}$

II Encryption

PlainText : $M < n$

CipherText : $C = M^e \pmod n$

III Decryption

Cipher Text : C

Plain Text : $M = C^d \pmod{n}$

* Conclusion

Thus RSA algorithm is used to implement asymmetric key cryptography.