Module 1 – RSA Encryption

RSA is an asymmetric cryptographic algorithm used by to encrypt and decrypt messages, It uses two different keys hence the asymmetry.

Algorithm steps

1.select to random prime numbers p,q (from the user)

2.calculate rsa modulus n = p\*q

3.calculate totient = (p-1) (q-1)

4.select public key e (Finding the first number that is co-prime with the totient)

5.select private key private d (using the inverse mod operation)

Input

* p
* q
* message to be encrypted

output

decrypted message

module 2 – sender, receiver

in this module the receiver generates the keys needed for encryption and decryption randomly then it communicates the public key to the sender through a .txt file named ‘public.txt’

the sender reads the public key and encrypts the message then uses another .txt file to send the message named ‘message.txt’ meanwhile the receiver is waiting for the existence of ‘message.txt’ to read the sent message and decrypts it using the private key.

Steps

Receiver

* Generate keys
* Write public key to file
* Wait for sender

Sender

* Read public key if exists else wait
* After reading encrypt message
* Send message

Module 3 – encryption time