# Aim:

**Language used: Python**

a. To implement RSA cryptosystem

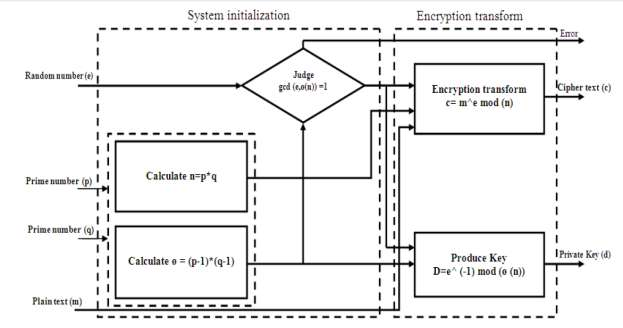
b. To implement a Digital signature scheme using El Gamal.

# Theory:

## What is public key cryptography?

Sometimes referred to as [asymmetric cryptography](http://searchsecurity.techtarget.com/definition/asymmetric-cryptography), public key cryptography is a class of cryptographic protocols based on algorithms. This method of cryptography requires two separate keys, one that is private or secret, and one that is public. Public key cryptography uses a pair of keys to encrypt and decrypt data to protect it against unauthorized access or use. Network users receive a public and private key pair from certification authorities. If other users want to encrypt data, they get the intended recipient’s public key from a public directory. This key is used to encrypt the message, and to send it to the recipient. When the message arrives, the recipient decrypts it using a private key, to which no one else has access.

## Block diagram of RSA algorithm



## Description of RSA algorithm

The [Rivest-Sharmir-Adleman (RSA) algorithm](http://searchsecurity.techtarget.com/definition/RSA) is the cryptography system that is used for public key cryptography, which is commonly used when sending secure, sensitive data over an insecure network like the internet. The [RSA algorithm](http://mathworld.wolfram.com/RSAEncryption.html) is popular because it allows both public and private keys to encrypt messages so their confidentiality and authenticity remain intact.

## Theoretically solve the RSA algorithm

## Need for digital signature

* Saves time  
  You no longer have to wait for your manager to return from a holiday or conference for that signature. Digital signatures ensure that businesses save on cost and time with documents and contracts signed off with a click of a button. There are huge savings in cost and time especially when the person required to sign is in a geographically different area. Documents can be signed off almost instantly, from anywhere. Be it a tablet, phone or computer, digital signatures can seamlessly ensure this otherwise tedious task is wrapped up in minutes.
* Cost savings  
  Many companies also see significant cost savings, with little or no expense in ink, paper, printing, scanning , shipping/delivery or travel expenses. There are also savings in other indirect costs such as filing, rekeying data, archiving, or tracking.
* Workflow efficiency  
  With lesser delays, digital signatures ensure better efficiency in workflow. Managing and tracking documents are made easier, with lesser effort and time involved. Many features of the digital signatures help speed up the work process. For instance, email notifications help remind the person to sign, while status tracking helps to know at which stage the document is at.
* Better customer experience  
  Digital signatures provide the convenience of signing important documents wherever a customer or the person to sign is located. Salespeople do not have to wait for the customer to come to the bank or office. Documents can be signed off at the doorstep. This is ideal, especially in remote areas and smaller townships providing improved and personalized services. The customer has the freedom to be anywhere, and engage with a company, making services and businesses far more easy, quick and user – friendly.
* Security  
  When it comes to signatures, authenticity and security is a priority. Digital signatures reduce the risk of duplication or alteration of the document itself. Digital signatures ensure that signatures are verified, authentic and legitimate. Signers are provided with PINs, passwords and codes that can authenticate and verify their identity and approve their signatures. Time stamping provides the date and time of the signature and thus provides a track of the document, minimising any risk of tampering or fraud. Security features embedded in digital signatures ensure that documents have not been altered without authorization.
* Legal validity  
  Digital signatures provide authenticity and ensure that the signature is verified. This can stand in any court of law like any other signed paper document. Time stamping and ability to track and easily archive documents improve and simplify audit and compliance.
* Future validity  
  Digital signatures also hold validity into the future. ETSI PDF Advanced Signatures (PAdES) with its eIDAS requirements have validity well into the future with its long term signature formats. Should there be far reaching technological changes, digital signatures would still be valid for the foreseeable future.
* Environmental benefits  
  As corporations and businesses become more conscious of their role in sustainability, digital signatures are a step ahead in their efforts in reducing waste and being environmentally friendly.
* Business efficiency  
  The costs involved in integrating digital signatures into the work processes is relatively small, compared to its benefits. With quicker contract turnaround time, and reduced the work flow time, digital signatures are ideal for both small and large organizations.

1. Solve Digital Signature using El Gamal algorithm

# Implementation:

|  |
| --- |
| import math as m  p=int(input("Enter a prime number p>>>>"))  q=int(input("Enter a prime number q>>>>"))  n=p\*q  phi=(p-1)\*(q-1)  print(phi)  e=0  for i in range(2,phi):  e=i  if(m.gcd(e,phi)==1 and (e!=p) and(e!=q)):  break  print("Public Key:"+str(e))  k=0  d=0  for i in range(1,10):  k=i  temp=((k\*phi)+1)/e  if(temp.is\_integer()==True):  d=temp  break  d=int(d)  print("Private Key:"+str(d))  m=int(input("Enter the Plaintext Number>>>"))  c=(m\*\*e)%n  print("Encrypted Cipher Text>>"+str(c))  p1=(c\*\*d)%n  print("Decrypted Plain Text>>"+str(p1))  print("--------------DIGITAL SIGNATURE--------------------")  a=int(input("Enter the Digital Signature>>>"))  c1=(a\*\*d)%n  print("Encrypted Cipher Digital Signature>>"+str(c1))  p11=(c1\*\*e)%n  print("Decrypted Plain Digital Signature>>"+str(p11)) |

# 

# Conclusion:

In this experiment we have successfully implemented the RSA cryptosystem and the Digital signature scheme using El Gamal.

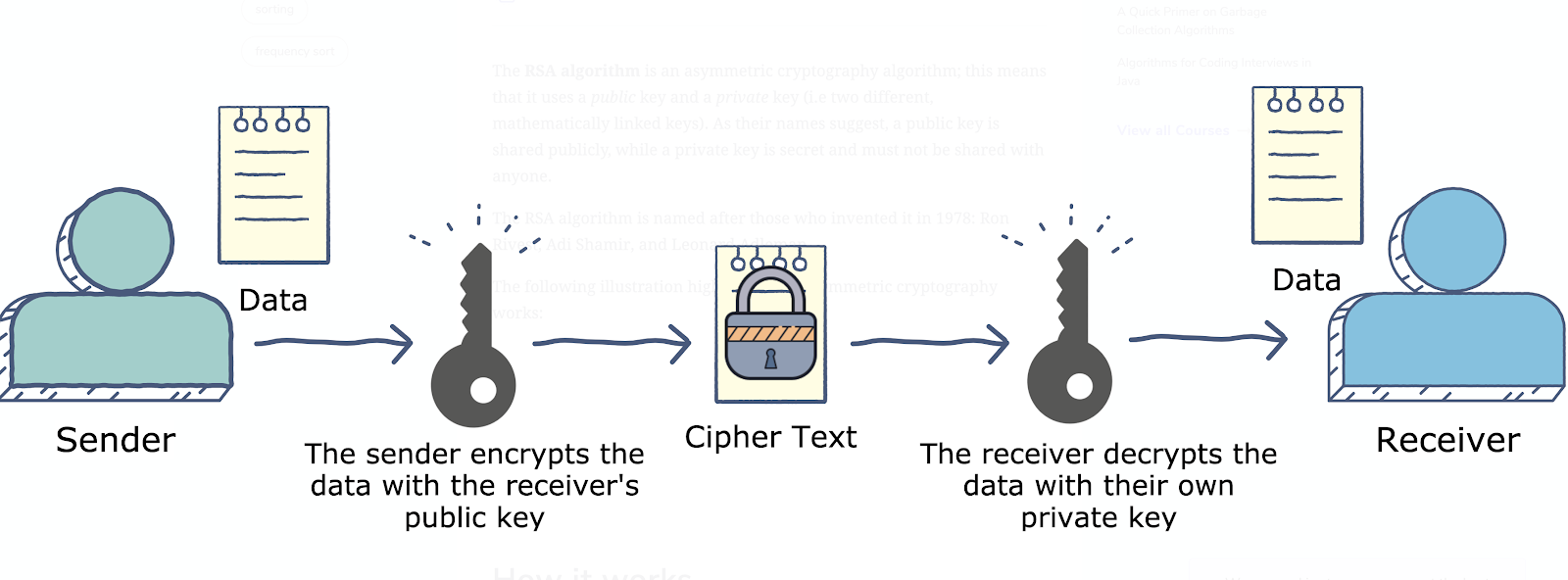
# Viva Questions:

## Explain the working of RSA algorithms.

The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.

The following illustration highlights how asymmetric cryptography works:



## **How it works**

The RSA algorithm ensures that the keys, in the above illustration, are as secure as possible. The following steps highlight how it works:

* Generating the keys
* Encryption
* Decryption

## What are the advantages of RSA algorithms? Explain with an example.

There are advantages and disadvantages of RSA algorithms. The advantages include; RSA algorithm is safe and secure for its users through the use of complex mathematics. The RSA algorithm is hard to crack since it involves factorization of prime numbers which are difficult to factorize. Moreover, the RSA algorithm uses the public key to encrypt data and the key is known to everyone, therefore, it is easy to share the public key.

## What are the disadvantages of RSA algorithms? Explain with an example

The disadvantages include; RSA algorithms can be very slow in cases where large data needs to be encrypted by the same computer. It requires a third party to verify the reliability of public keys. Data transferred through the RSA algorithm could be compromised through middlemen who might temper with the public key system. In conclusion, both the symmetric encryption technique and the asymmetric encryption technique are important in encryption of sensitive data.