Assignment Number: 4

Name: Divya Shah; Branch: I.T (T.E.); Roll Number: 115 24/08/2023

**Aim:** Implementation and analysis of RSA cryptosystem and Digital signature scheme

using RSA.

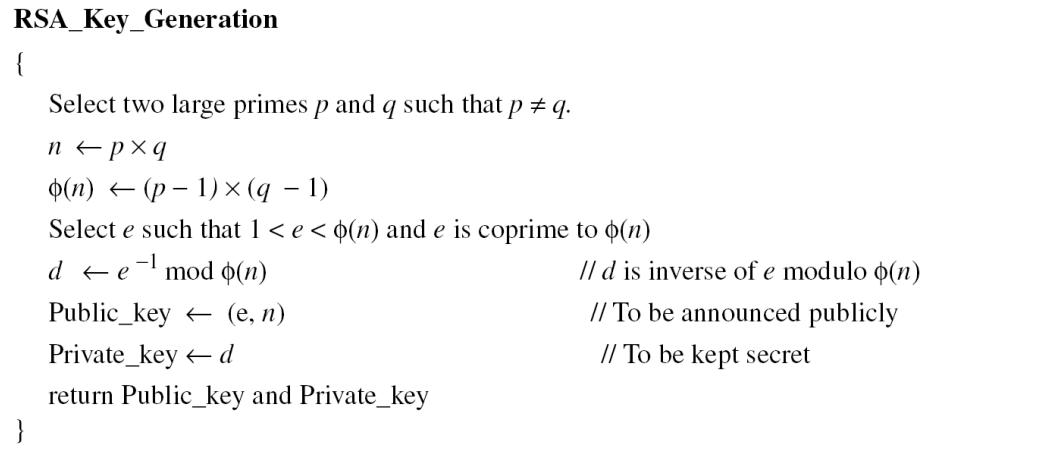
**LO mapped:** LO2

**Theory:**

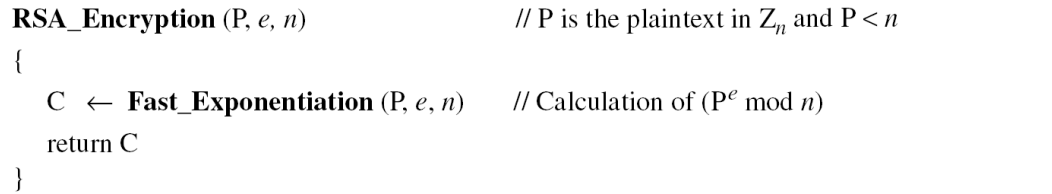
RSA (Rivest Shamir Adleman Algorithm):

Asymmetric cryptography plays a pivotal role in securing modern communication. The RSA cryptosystem stands as a cornerstone in this field, providing a foundation for secure data transmission and digital signatures. This assignment aims to explore the implementation and analysis of RSA encryption and its application in digital signature schemes.

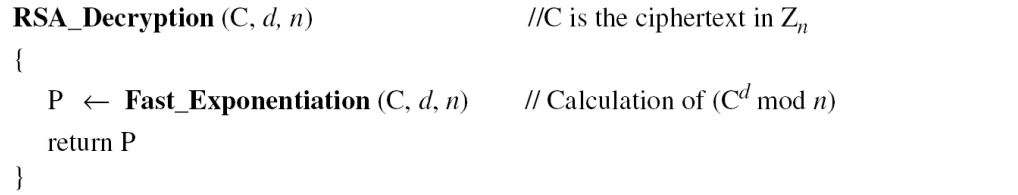
Steps of RSA:



Encryption is given as:



Decryption is given as:



Digital Signature:

A Digital Signature is an authentication mechanism that enables the creator of the message to attack a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

|  |
| --- |
|  |

**Conclusion:** By this assignment we learned RSA algorithm and made digital signature using RSA algorithm.