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:

```
RSA_Key_Generation
{
   Select two large primes p and q such that p ≠ q.
   n ← p × q
   ϕ(n) ← (p − 1) × (q − 1)
   Select e such that 1 < e < ϕ(n) and e is coprime to ϕ(n)
   d ← e^−1 mod ϕ(n)                    // d is inverse of e modulo ϕ(n)
   Public_key ← (e, n)                  // To be announced publicly
   Private_key ← d                      // To be kept secret
   return Public_key and Private_key
}
```

Encryption is given as:

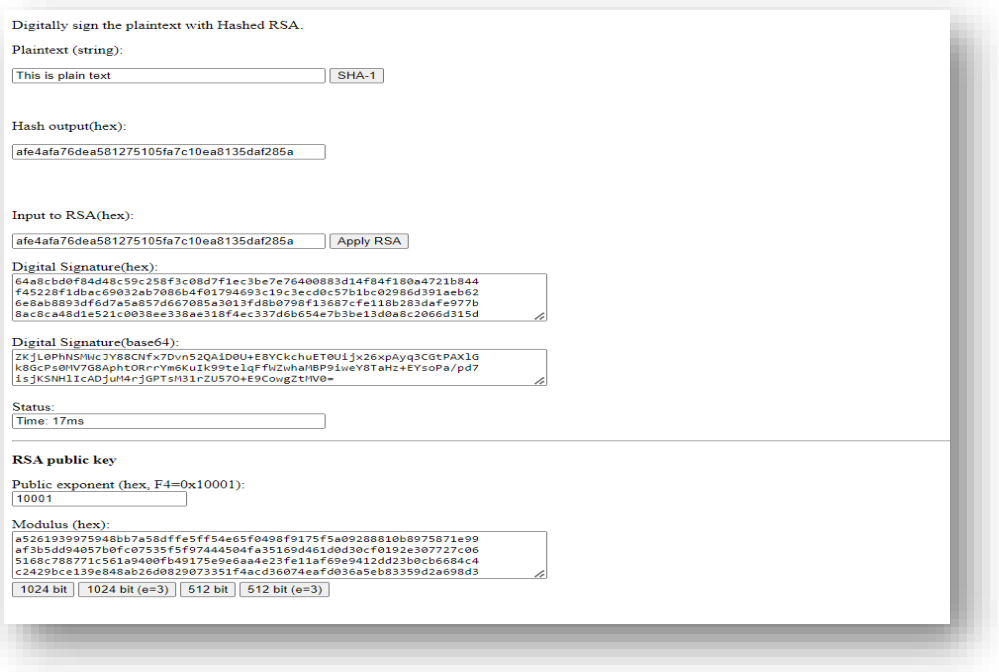
```
RSA_Encryption (P, e, n)                // P is the plaintext in Z_n and P < n
{
   C ← Fast_Exponentiation (P, e, n)    // Calculation of (P^e mod n)
   return C
}
```

Decryption is given as:

```
RSA_Decryption (C, d, n)                //C is the ciphertext in Z_n
{
   P ← Fast_Exponentiation (C, d, n)    // Calculation of (C^d mod n)
   return P
}
```

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.