Assignment 3

Aim:- Implementation and analysis of RSA cryptosystem and Digital Signature scheme using RSA

Lo Mapped:- Lo2

Theory :- RSA (Rivest-Shamir-Adleman):-

RSA is a widely used public-key cryptosystem for secure data transmission and digital signatures. It's based on the mathematical properties of large prime numbers. RSA involves a pair of keys: a public key for encryption and a private key for decryption. The security of RSA relies on the difficulty of factoring large semiprime numbers.

Algorithm:-

1. Key Generation:

   - Choose two distinct prime numbers, p and q.

   - Calculate n = p * q.

   - Compute the totient φ(n) = (p - 1) * (q - 1).

   - Choose an integer e (usually a small prime, commonly 65537) that is coprime with φ(n).

   - Compute d such that (d * e) % φ(n) = 1.

   - Public key: (e, n)

   - Private key: (d, n)

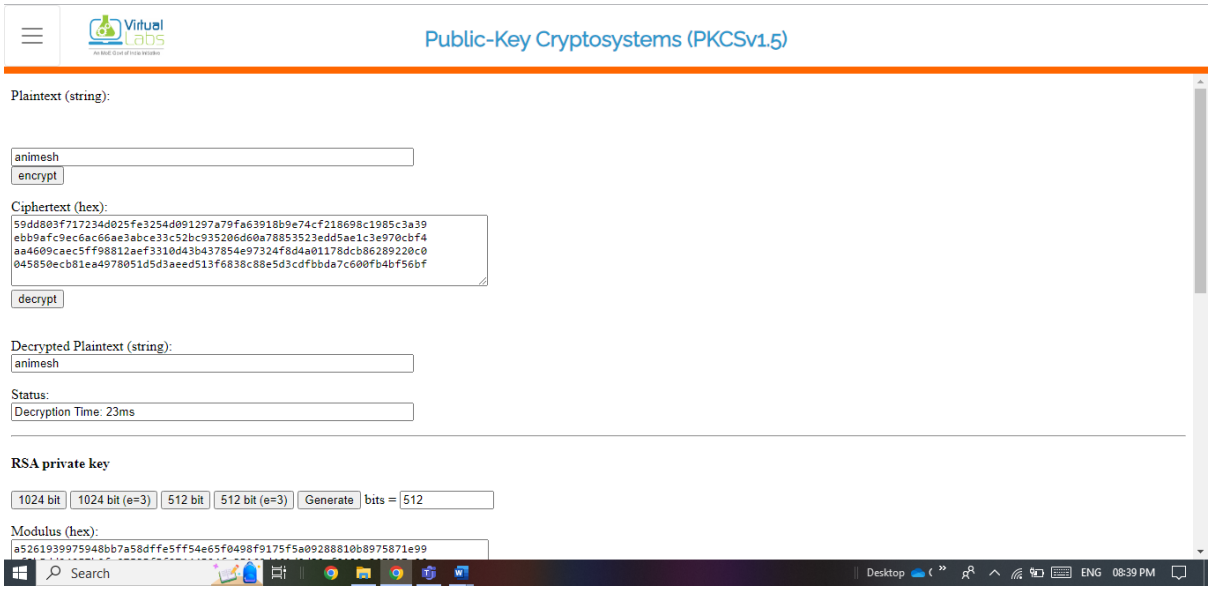
2. Encryption:

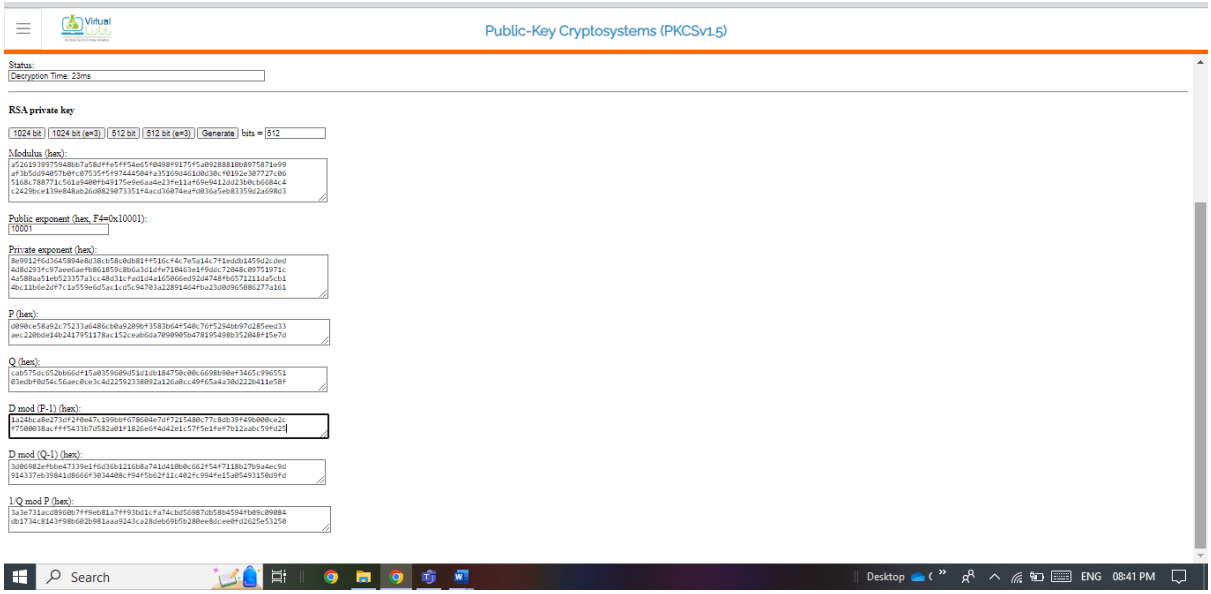
   - Convert the plaintext message into a numeric value m.

   - Compute the ciphertext c = (m^e) % n.

3. Decryption:

   - Compute the plaintext message m = (c^d) % n.





Digital Signature:-

A digital signature is a cryptographic technique that provides authenticity, integrity, and non-repudiation for digital messages or documents. It involves using a private key to sign the message and a public key to verify the signature. Digital signatures ensure that the sender of a message is authenticated and that the message has not been tampered with during transmission.

Algorithm:-

1. Key Generation:

   - Choose a private key for signing.

   - Compute a corresponding public key for verification.

2. Signing:

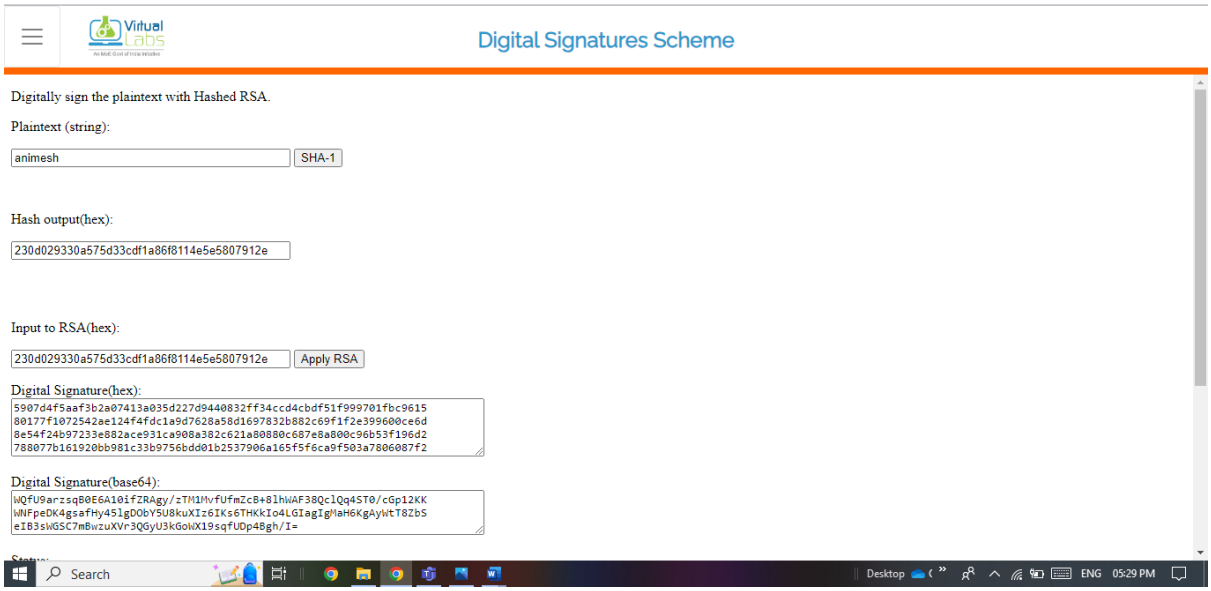
   - Hash the message to produce a fixed-length digest.

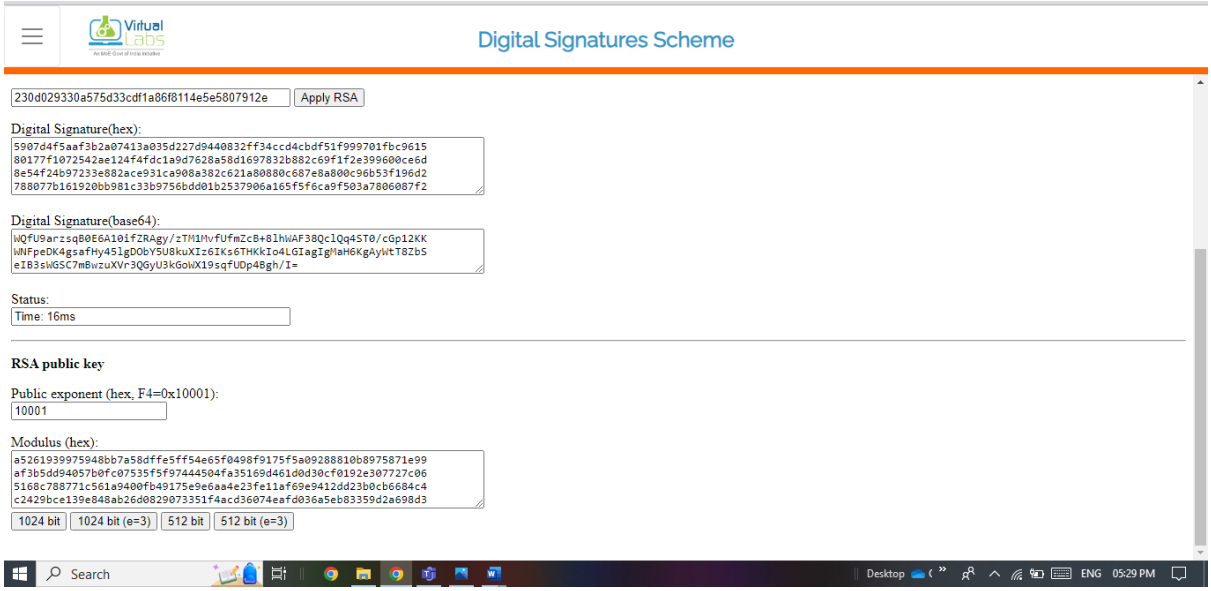
- Encrypt the digest using the private key to create the digital signature.

3. Verification:

- Decrypt the digital signature using the sender's public key to get the digest.
- Hash the received message to produce a digest.
- Compare the two digests. If they match, the signature is valid.

Digital signatures are essential for secure communication, online transactions, and authentication of digital documents.





Conclusion:- Thus we learnt and implemented RSA and digital signature using RSA