EXPERIMENT NO. 7

AIM: Implementation and analysis of RSA cryptosystem.

REQUIREMENTS: Virtual Lab

THEORY:

RSA (Rivest-Shamir-Adleman) is a widely used public-key cryptosystem that enables secure communication over an insecure network. It is an asymmetric encryption algorithm, meaning it uses two different keys:

- Public Key: Used for encryption and can be shared openly.
- Private Key: Used for decryption and must be kept secret.

The security of RSA is based on the mathematical difficulty of factoring large prime numbers, making it a strong encryption method for secure data exchange.

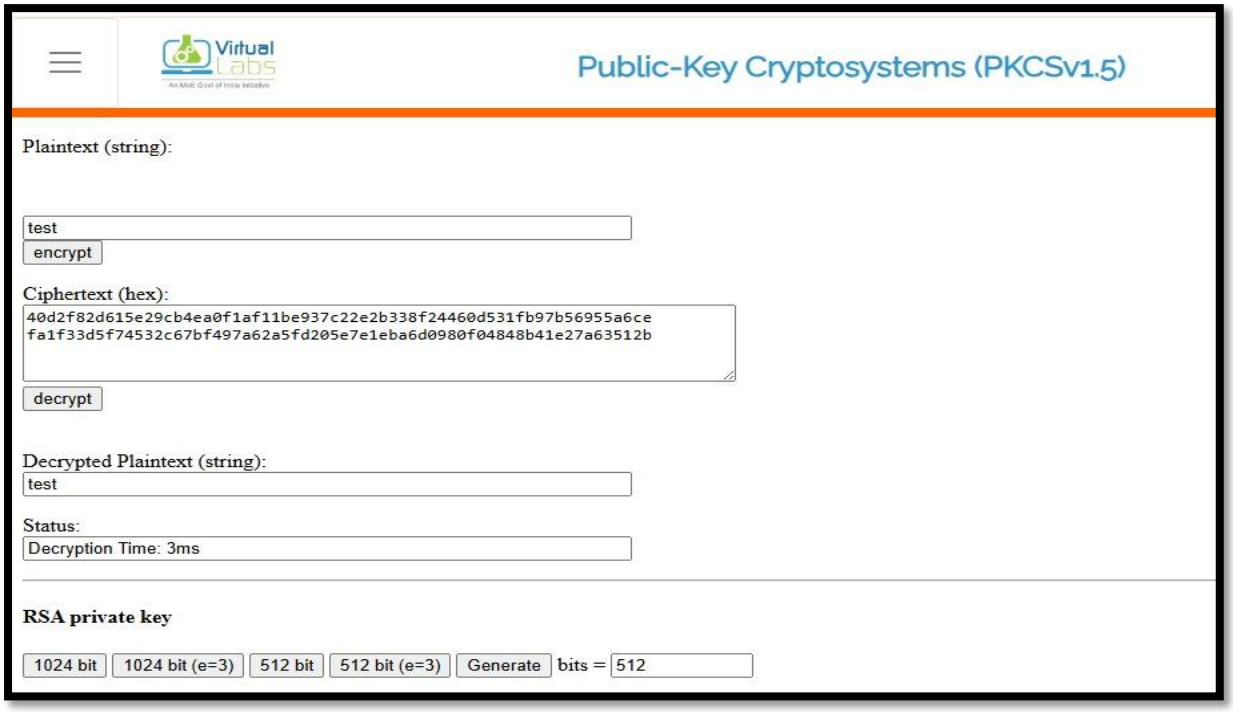
PROCEDURE:

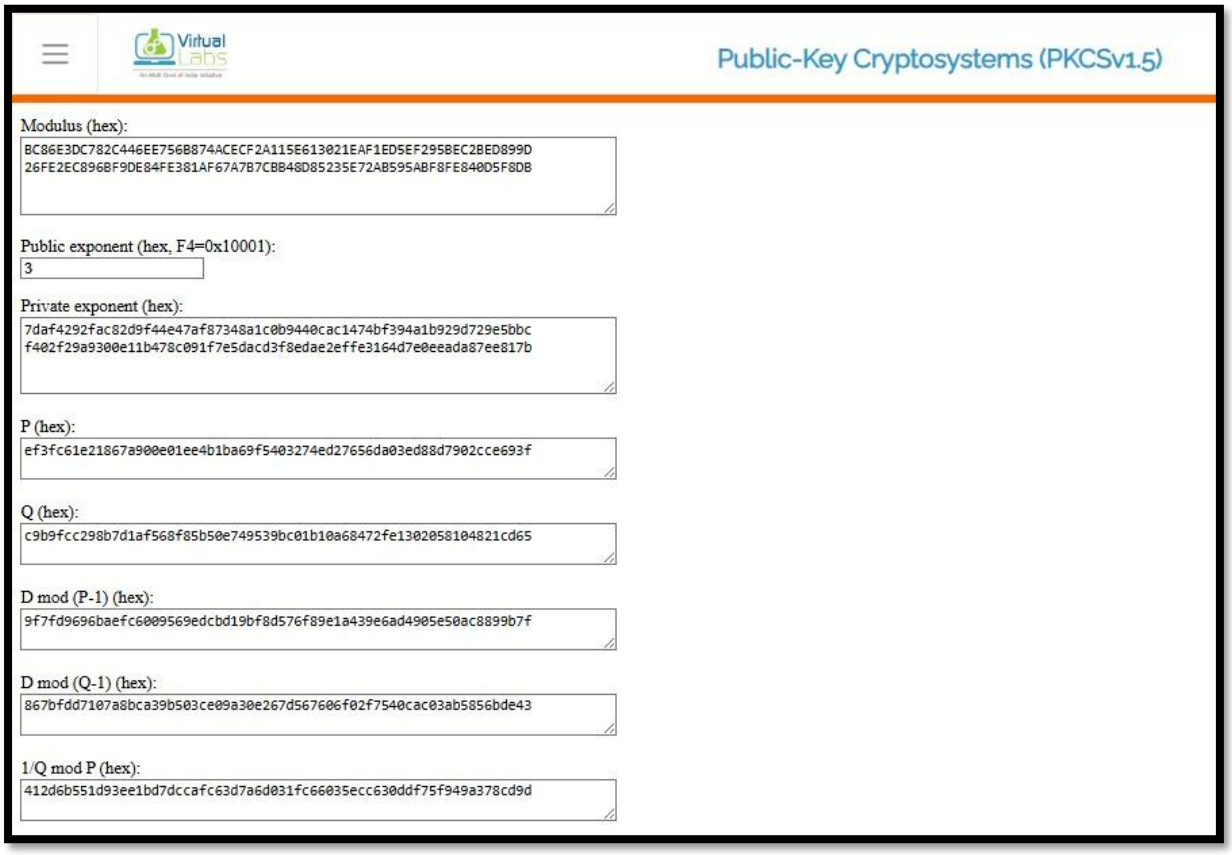
Step 1 : Enter the input text to be encrypted in the 'Plaintext' area

Step 2 : Select keysize of public key from **RSA Private key** section by clicking on one of the key button.

Step 3 : Click on **encrypt** button to generate a ciphertext.

RESULT:





ASSIGNMENT:

Q1: Let p = 17, q = 11 and N = pq. If (in the public-key) e= 7, then a possible value for the trap-door d (in the private-key) in an RAS cryptosystem is….
A: 23

Q2: Encrypt the message m = 57 with the textbook RSA with the public key pk = N= 253, e = 3…

A: 196

Q3: In Asymmetric-Key cipher, the sender uses the _____ key
A: Public Key

Q4: Why PKCSv1.5 is more secure?

A: PKCSv1.5 improves security by using padding to prevent attacks like Bleichenbacher's attack, adding randomness, and strengthening RSA encryption in SSL/TLS. It protects against chosen ciphertext attacks and ensures safer cryptographic implementations.

CONCLUSION:

In this experiment, we successfully implemented and analyzed the RSA cryptosystem. We explored the key generation process, encryption, and decryption mechanisms. The experiment demonstrated how RSA ensures secure communication using asymmetric encryption, where the public key is used for encryption and the private key for decryption. Additionally, we examined the importance of key sizes and security enhancements like PKCS1 v1.5. The results validate that RSA is an effective and widely used cryptographic algorithm for secure data transmission**.**