

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:

The screenshot displays the Virtual Labs interface for Public-Key Cryptosystems (PKCSv1.5). The interface includes a header with the Virtual Labs logo and the title 'Public-Key Cryptosystems (PKCSv1.5)'. The main content area is divided into several sections:

- Plaintext (string):** A text input field containing 'test' and an 'encrypt' button.
- Ciphertext (hex):** A text output field displaying the hexadecimal ciphertext: '40d2f82d615e29cb4ea0f1af11be937c22e2b338f24460d531fb97b56955a6cefa1f33d5f74532c67bf497a62a5fd205e7e1eba6d0980f04848b41e27a63512b'. Below this field is a 'decrypt' button.
- Decrypted Plaintext (string):** A text output field displaying 'test'.
- Status:** A text output field displaying 'Decryption Time: 3ms'.
- RSA private key:** A section with buttons for '1024 bit', '1024 bit (e=3)', '512 bit', and '512 bit (e=3)', followed by a 'Generate' button and a 'bits =' field set to '512'.



Virtual
Labs

An e-Learning Environment for All

Public-Key Cryptosystems (PKCSv1.5)

Modulus (hex):

BC86E3DC782C446EE756B874ACECF2A115E613021EAF1ED5EF2958EC2BED899D
 26FE2EC8968F9DE84FE381AF67A7B7CBB48D85235E72AB595ABF8FE840D5F8DB

Public exponent (hex, F4=0x10001):

3

Private exponent (hex):

7daf4292fac82d9f44e47af87348a1c0b9440cac1474bf394a1b929d729e5bbc
 f402f29a9300e11b478c091f7e5dacd3f8edae2effe3164d7e0eeada87ee817b

P (hex):

ef3fc61e21867a900e01ee4b1ba69f5403274ed27656da03ed88d7902cce693f

Q (hex):

c9b9fcc298b7d1af568f85b50e749539bc01b10a68472fe1302058104821cd65

D mod (P-1) (hex):

9f7fd9696baefc6009569edcbd19bf8d576f89e1a439e6ad4905e50ac8899b7f

D mod (Q-1) (hex):

867bfdd7107a8bca39b503ce09a30e267d567606f02f7540cac03ab5856bde43

1/Q mod P (hex):

412d6b551d93ee1bd7dccaafc63d7a6d031fc66035ecc630ddf75f949a378cd9d

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 RSA 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.