TIT–704

B. TECH. (CSE)
(SEVENTH SEMESTER)
MID SEMESTER EXAMINATION, 2022
CRYPTOGRAPHY AND NETWORK SECURITY

Time : 1½ Hours

Maximum Marks : 50

Note : (i) Answer all the questions by choosing any *one* of the sub-questions.

(ii) Each question carries 10 marks.

1. (a) Define Cryptography and its benefits. Explain conventional encryption model.

(CO1)

OR

(b) Write short notes on the following : (CO1)

(i) Security services

(ii) Security attacks

P. T. O.

2. (a) Perform the encryption and decryption using RSA algorithm for the following :

(CO1, CO2)

$P = 7; q = 11; e = 17; M = 8.$

OR

(b) What are the classical encryption techniques ? Explain Steganography and Cryptanalysis.   (CO1, CO2)

3. (a) Apply Caesar cipher and $K = 5$ decrypt the given Ciphertext :   (CO1, CO2)

"YMJTYMJWXNIJTKXNQJSHJ"

OR

(b) Explain principles of block ciphers, with its different modes of operation and example.   (CO1, CO2)

4. (a) Explain Pseudo random number generation using Linear Congruential and Blum BlumShub algorithms. (CO1, CO2)

OR

(b) Explain Shannon's theory of confusion and diffusion.   (CO1, CO2)

5. (a) Explain the *two* basic functions used in encryption algorithms. Explain with the help of an example. (CO1, CO2)

OR

(b) What are the operations used in AES (Advanced Encryption Standard) ?

(CO1, CO2)