H Roll No. .....

TIT–704

B.TECH. (CSE)
(SEVENTH SEMESTER)
MID SEMESTER
EXAMINATION, Oct., 2023

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 sub-question carries 10 marks.

1. (a) Define Cryptography and its benefits. Explain the Conventional encryption model. (CO1, CO2)

OR

(b) Explain the significance of each parameter in the RSA Algorithm. (CO1, CO2)

P. T. O.

2. (a) Perform encryption and decryption using the 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 :

"ZKJTYMJHXMKITKXNQJSHJ". (CO1, CO2)

OR

(b) Explain the principles of block ciphers, with their different models of operation and examples. (CO1, CO2)

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

OR

(b) Provide examples of cryptographic algorithms that incorporate the principles 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) Describe different modes of operation for block ciphers, providing examples of ECB, CBC, OFB, and CFB. (CO1, CO2)