Code No: **20CC5O01/20CC5T01**

R20

III B. TECH I SEMESTER REGULAR EXAMINATIONS, NOVEMBER - 2022
CRYPTOGRAPHY AND NETWORK SECURITY
(Common to CIC and AID)

Time: 3 Hours **Max. Marks: 70**

Note : Answer **ONE** question from each unit **(5 × 14 = 70 Marks)**

~~~~~~

UNIT-I

1. a) List the security services and describe the role of each service in network communication. [7M]

   b) Construct a Caesar cipher and convert the word “the Network security” into cipher text with k=3. [7M]

(OR)

2. a) Differentiate between passive attacks and active attacks. [7M]

   b) Briefly define the monoalphabetic cipher. [7M]

UNIT-II

3. a) Explain any two cipher block modes of operation. [7M]

   b) Explain single round of DES algorithm. [7M]

(OR)

4. Explain AES algorithm in detail. [14M]

UNIT-III

5. a) Explain the algorithm for generating keys in RSA algorithm. Perform encryption and decryption using RSA Algorithm for the following. P=7; q=11; e=13; M=8. [7M]

   b) Illustrate man in the middle attack on Diffie Hellman key exchange algorithm. [7M]

(OR)

6. a) Consider a Diffie-Hellman Scheme with a common prime q=11 and a primitive root α=2. [7M]

      i) If user A has public key Y_A=9, What is A's private key X_A?
      ii) If user B has public key Y_B=3, What is the shared secret key K?

   b) Explain public key cryptography and its characteristics. [7M]

UNIT-IV

7. a) List the steps to generate digital signature using Digital Signature Standard (DSS). [7M]

   b) Illustrate the requirements of Message Authentication codes. [7M]

(OR)
~~~~~~

8. a) Compare and contrast the principal differences between version 4 and version 5 of Kerberos. [4M]

   b) Outline the features of SHA-512 algorithm. [10M]

UNIT-V

9. a) Explain about PGP key management in E-mail protection. [7M]

   b) Explain about ESP format in IP security. [7M]

(OR)

10. a) Explain about SSL handshake protocol. [7M]

    b) Explain the modes of IPSEC protocol. [7M]

* * * * *