



CBCS SCHEME

21CS733

Seventh Semester B.E./B.Tech. Degree Examination, June/July 2026 Cryptography and Network Security

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

- 1 a. Illustrate Symmetric Cipher Model in detail. (08 Marks)
- b. Perform Encryption and Decryption on plaintext "CRYPTOGRAPHY" using HILL Cipher technique with key matrix, $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ (08 Marks)
- c. Explain cryptanalysis and Brute force Attack. (04 Marks)

OR

- 2 a. With neat diagram, explain Fiestal Encryption and Decryption Algorithm. (10 Marks)
- b. Draw and explain DES Standard Algorithm. (06 Marks)
- c. Distinguish between Block Cipher and Stream Cipher. (04 Marks)

Module-2

- 3 a. Explain Public-key cryptosystem. (10 Marks)
- b. Perform Encryption, decryption using RSA algorithm.
 - (i) $P = 11, q = 13, e = 11, m = 7$
 - (ii) $P = 3, q = 11, e = 7, m = 5$ (10 Marks)

OR

- 4 a. User A and B use the Diffie-Hellman key Exchange technique with common prime number $q = 353$ and primitive root $\alpha = 3$, calculate the keys,
 - (i) If user A has private key $X_A = 97$, what is A's public key Y_A ?
 - (ii) If user B has private key $X_B = 233$, what is B's public key Y_B ? (10 Marks)
- b. Explain with example Elgamal cryptographic systems. (10 Marks)

Module-3

- 5 a. Explain key distribution scenario with neat diagram. (10 Marks)
- b. Explain decentralized key control and controlling key usage in symmetric key distribution using symmetric encryption. (10 Marks)

OR

- 6 a. With neat diagram, explain secret key distribution with confidentiality and authentication. (10 Marks)
- b. Explain different schemes of distribution of public keys. (10 Marks)

Module-4

- 7 a. Illustrate the General Format of X.509 certificate. (10 Marks)
- b. Describe public key infrastructure with neat diagram. (10 Marks)

OR

- 8 a. Explain Remote User Authentication principles. (10 Marks)
- b. Explain overview of Kerberos with diagram. Explain Kerberos exchanges. (10 Marks)

Module-5

- 9 a. Write a note on PGP (Pretty Good Privacy) services and notations. (10 Marks)
- b. List and explain MIME content type and transfer encoding. (10 Marks)

OR

- 10 a. Describe the application and benefits of IPsec. (10 Marks)
- b. Explain Internet Key Exchange (IKE) Key Determination features. (10 Marks)

* * * * *