EPCET LIBRARY BANGALORE-49

CBCS SCHEME

USN | | | | | | | | | | |

21IS71

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.

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-1

1 a. Explain with a neat diagram the Symmetric Cipher Model and demonstrate the working of Caesar Cipher Encryption and decryption on the plain text "VISVESVARAYA". **(10 Marks)**

b. Explain with neat diagram Fiestel Cipher Structure. **(10 Marks)**

OR

2 a. Using Playfair cipher technique encrypt the plain text "ATTACK" taking the key as "MONARCHY". **(10 Marks)**

b. Explain with a neat diagram the single round function in DES Encryption Model. **(10 Marks)**

Module-2

3 a. Explain with a neat diagram Public Key Cryptosystem. **(10 Marks)**

b. Solve using Diffie Hellman key exchange technique with common prime q = 17 and primitive root $\alpha = 7$
(i) Find A's public key Y_A if user A has private key $X_A = 5$
(ii) Find B's public key Y_B if user B has private key $X_B = 12$ **(10 Marks)**

OR

4 a. Explain the process of Elagamal Crypto System and man-in the middle attack. **(10 Marks)**

b. Perform encryption and decryption using RSA algorithm for p = 3, q = 11, e = 7 and M = 31 **(10 Marks)**

Module-3

5 a. Explain with a neat diagram key distribution scenario and highlight the importance of hierarchical key control and session key lifetime. **(10 Marks)**

b. With a neat diagram explain Transparent Key Control Scheme and Decentralized Key Control. **(10 Marks)**

OR

6 a. Explain simple secret key distribution and secret key distribution with confidentiality and authentication. **(10 Marks)**

b. Explain in detail the general scheme for distribution of public keys. **(10 Marks)**

Module-4

7 a. Explain X.509 Certificate format in detail. **(10 Marks)**

b. With a neat diagram explain PKIX Architectural Model and its management functions. **(10 Marks)**

OR

8 a. Explain the process of Mutual Authentication in remote user authentication using symmetric encryption. **(10 Marks)**

b. Explain Kerberos Version 4 message exchanges. **(10 Marks)**

Module-5

9 a. Explain with a neat diagram Encapsulating security payload format. **(10 Marks)**

b. Explain the Transport and Tunnel Modes in IPsec. **(10 Marks)**

OR

10 a. Explain PGP cryptographic function with a neat diagram. **(10 Marks)**

b. Explain IKE header and payload formats. **(10 Marks)**

* * * * *

VTU-27-05-2026 08:41:18am
27-05-2026 09:01:06am
EP - EP - EP -