CBCS SCHEME

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

21IS71

Seventh Semester B.E./B.Tech. Degree Examination, Dec.2025/Jan.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. Describe Playfair Cipher Algorithm. Find the Ciphertext for plaintext " instruments" with Key = " MONARCHY". **(10 Marks)**

b. Describe Hill Cipher Algorithm. Using Hill-Cipher algorithm perform Encryption and Decryption for the plaintext = " Paymoremoney". Given,

$$\text{Key} \rightarrow K = \begin{bmatrix} 17 & 7 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \& K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$ **(10 Marks)**

OR

2 a. Illustrate with neat diagram Fiestel Cipher Structure for Encryption and Decryption. **(10 Marks)**

b. Illustrate with neat diagram DES Encryption algorithm. **(10 Marks)**

Module-2

3 a. Differentiate Public Key Encryption and Conventional Encryption. **(04 Marks)**

b. Describe the steps of RSA algorithm. Using RSA algorithm, derive public key, private key and perform Encryption and decryption for message M = 9.
Assume p = 3, q = 11, e = 3. **(10 Marks)**

c. With neat diagram, explain authentication and secrecy in Public Key Cryptosystem. **(06 Marks)**

OR

4 a. Explain Diffie – Hellman Key Exchange algorithm. Users A & B use Diffie – Hillman Key Exchange technique, common prime q = 11 and prime time root alpha (α) = 7.
i) If user A has private key $X_A = 3$. What is A's public key Y_A?
ii) If user B has private key $X_B = 6$. What is B's public key Y_B?
iii) What is the Shared Secret Key? **(10 Marks)**

b. Discuss Elgamal Crypto System. Perform encryption and decryption using
q = 19, alpha(α) =10, k = 6, M = 17, $X_A = 5$, $Y_A = 3$. **(10 Marks)**

Module-3

5 a. Illustrate Symmetric Key Distribution using Symmetric Encryption involving KDC. **(08 Marks)**

b. Explain Transparent Key Control Scheme. **(07 Marks)**

c. Write a note on Session Key Lifetime. **(05 Marks)**

OR

6 a. Illustrate secret key distribution with confidentiality and authentication using asymmetric encryption. **(07 Marks)**

b. Define Control Vector. Explain the coupling and Decoupling process of control vectors. **(07 Marks)**

c. Illustrate the distribution of Public Key with respect to Public – key Authority. **(06 Marks)**

Module-4

7 a. With neat diagram explain the general format of X.509 certificate, along with notation to define a certificate. **(10 Marks)**

b. With neat diagram bring out the relationship among the key elements of PKIX Model along with PKIX management functions. **(10 Marks)**

OR

8 a. Explain Kerberos Version 5 message exchange with neat diagram. **(10 Marks)**

b. Illustrate Mutual authentication and one way authentication with respect to remote user authentication using Symmetric Encryption. **(10 Marks)**

Module-5

9 a. Describe in detail PGP (Pretty Good Privacy) Cryptographic functions. **(10 Marks)**

b. List the Limitations of SMTP scheme. **(04 Marks)**

c. List the elements of MIME and describe the various header fields defined in MIME. **(06 Marks)**

OR

10 a. Illustrate the IP traffic processing for outbound and inbound packets. **(10 Marks)**

b. With a neat diagram explain the top level format of ESP packet and also the substructure of payload data. **(10 Marks)**

* * * * *