CBCS SCHEME

USN | | | | | | | | | |

21CS733

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. Explain simplified model of symmetric encryption scheme. **(04 Marks)**

b. Construct a playfair matrix with the key "MONARCHY" and find the ciphertext for the plaintext "Instruments". **(06 Marks)**

c. With a neat diagram, explain Feistel encryption and decryption. **(10 Marks)**

OR

2 a. Explain Hill cipher algorithm, using Hill cipher perform encryption and decryuption for Plaintext = "Pay more money" using key $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$. **(10 Marks)**

b. Explain encryption and decryption equations of vigenere cipher. Perform encryption using autokey system for the following :
Plainetext : "We are discovered save yourself"
Keyword : deceptive. **(10 Marks)**

Module-2

3 a. Differentiate conventional encryption and public – key encryption. **(04 Marks)**

b. Explain public key cryptosystem to provide authentication. **(06 Marks)**

c. Explain RSA algorithm. Using RSA perform encryption and decryption using P = 17, q = 11, e = 7 and M = 88. **(10 Marks)**

OR

4 a. Explain Man-in-the middle attack. **(10 Marks)**

b. Explain Elgamal cryptosystem. Perform encryption and decryption using q = 19, $\alpha = 10$, k = 6, M = 17, $X_A = 5$. **(10 Marks)**

Module-3

5 a. With a neat diagram explain key distribution scenario. **(08 Marks)**

b. Define Master key and session key. Explain the step involved in key distribution with confidentiality and authentication. **(12 Marks)**

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.

OR

6 a. Explain different techniques used for the distribution of public keys. **(10 Marks)**
b. Explain transparent key control scheme with neat diagram. **(10 Marks)**

Module-4

7 a. Explain X.509 certificate formats. **(10 Marks)**
b. Briefly explain Kerberos versions and message exchanges. **(10 Marks)**

OR

8 a. Explain mutual authentication with respect to remote user authentication. **(10 Marks)**
b. With a neat diagram explain PKIX architectural model. **(10 Marks)**

Module-5

9 a. Explain S|MIME functionality. **(10 Marks)**
b. Explain PGP (Pretty Good Privacy) cryptographic functions. **(10 Marks)**

OR

10 a. Explain IP security architecture with neat diagram. Also write the benefits of IP Sec. **(10 Marks)**
b. What are the fields of ESP packet format? Explain. Also differentiate transport and tunnel mode of encryption. **(10 Marks)**

* * * * *