CBCS SCHEME

USN | | | | | | | | | | | **21CS733**

Seventh Semester B.E./B.Tech. Degree Examination, June/July 2025

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 Feistel Cipher structure encryption and decryption with neat diagram. **(10 Marks)**

b. Explain polyalphabetic cipher. Find the cipher text for plaintext = "I am here now" and key = "when" using Vigenere cipher. **(10 Marks)**

OR

2 a. Explain play fair cipher algorithm. Find the cipher text for plaintext = "HERIGO" and key = "TODAY". **(10 Marks)**

b. Explain with neat diagram DES encryption algorithm. **(10 Marks)**

Module-2

3 a. With a neat sequence diagram explain how the Diffie-Hellman key exchange is insecure against Man-in-the Middle Attack. **(10 Marks)**

b. Explain RSA algorithm in detail. Perform encryption of plaintext and decryption of cipher text using RSA algorithm for $p = 11$, $q = 3$, $e = 3$ and $M = 4$. **(10 Marks)**

OR

4 a. With a neat diagram explain authentication and secrecy in public key cryptosystem. **(10 Marks)**

b. Explain Diffie-Hellman key exchange algorithm. Apply Diffie-Hellman key exchange algorithm for $q = 7$, primitive root $\alpha = 3$ $X_A = 4$, $X_B = 5$. Calculate the shared secret key. **(10 Marks)**

Module-3

5 a. Explain the distribution of public keys using public key certificates. **(10 Marks)**

b. With a neat diagram explain key distribution scenario. **(10 Marks)**

OR

6 a. Explain the distribution of public keys using public-key authority. **(10 Marks)**

b. Explain with neat diagram control vector encryption and decryption. **(10 Marks)**

Module-4

7 a. Explain X.509 certificate format. **(10 Marks)**

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

OR

8 a. Explain Kerberos version 5 message exchanges. **(10 Marks)**

b. Explain PKIX Architectural model. **(10 Marks)**

Module-5

9 a. With neat diagram discuss the sequence of steps for authentication and confidentiality in PGP. **(10 Marks)**

b. Discuss MIME content type and transfer encoding specifications. **(10 Marks)**

OR

10 a. Depict and explain the IPsec architecture. **(10 Marks)**

b. Explain the top level format and substructure of payload data for an ESP packet. **(10 Marks)**

* * * * *