CBCS SCHEME

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

18EC744

Seventh Semester B.E. Degree Examination, Dec.2024/Jan.2025
Cryptography

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Apply Euclidean Algorithm with an example for calculating the GCD of two numbers. **(10 Marks)**

b. Encrypt using 'Ceaser' cipher for the following plaintext message "Logic design" with key length = 3. **(05 Marks)**

c. Write the necessary steps involved for encryption in playfair method. **(05 Marks)**

OR

2 a. Encrypt the plain text 'HAND' using hill cipher with key $\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$ also decrypt it and verify the encryption and decryption. **(10 Marks)**

b. Elaborate rail fence cipher technique with example. **(05 Marks)**

c. Elaborate VIGENERE cipher technique with example. **(05 Marks)**

Module-2

3 a. Elaborate Feistel cipher structure with neat block diagram. **(10 Marks)**

b. Elaborate single round DES algorithm with block diagram. **(10 Marks)**

OR

4 a. Elaborate the general depiction of DES encryption algorithm. **(10 Marks)**

b. Explain AES encryption and decryption in detail. **(10 Marks)**

Module-3

5 a. Explain Groups, Rings and Fields. **(10 Marks)**

b. Write a note on prime numbers. **(05 Marks)**

c. Explain Fermat's theorem. **(05 Marks)**

OR

6 a. Write a short note on discrete logarithm. **(10 Marks)**

b. Explain Euler's totient function with example. **(10 Marks)**

Module-4

7 a. Explain the principle of public key cryptosystem. **(10 Marks)**

b. Explain in detail the RSA algorithm. **(10 Marks)**

OR

8 a. Explain Diffie Hellman key exchange algorithm. **(10 Marks)**

b. Write a note on elliptic curve cryptography. **(05 Marks)**

c. Perform the encryption and decryption using RSA algorithm for the following:
p = 11, q = 13, e = 7, M = 9 **(05 Marks)**

Module-5

9 a. Write a note on Linear Feedback Shift Registers. **(10 Marks)**

b. Explain the design and analysis of stream cipher. **(10 Marks)**

OR

10 a. Explain stream cipher using LFSRs. **(10 Marks)**

b. Explain GIFFORD with diagram. **(05 Marks)**

c. Explain PKZIP. **(05 Marks)**

* * * * *