CBCS SCHEME

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

18EC744

Seventh Semester B.E/B.Tech. Degree Examination, Dec.2025/Jan.2026
Cryptography

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Explain the model of symmetric cryptosystem with a neat diagram. **(06 Marks)**

b. Decrypt a message "PFOGOANPGXFX" using Hill cipher with a key

$$K = \begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix}$$ **(10 Marks)**

c. Explain Caesar cipher with an example. **(04 Marks)**

OR

2 a. Encrypt the plain text "CRYPTOGRAPHY" using playfair cipher with a key "HILL CIPHER", also give rules for encryption. **(06 Marks)**

b. Find the greatest common divisor (2740, 1760) using Euclidian algorithm and explain the algorithm. **(10 Marks)**

c. List out the properties of modular arithmetic for integer in Z_n. **(04 Marks)**

Module-2

3 a. With the help of a block diagram explain DES encryption algorithm. **(10 Marks)**

b. Briefly describe shift rows with an example in AES algorithm. **(04 Marks)**

c. Explain the parameters and design features of Feistel network. **(06 Marks)**

OR

4 a. Explain AES encryption process with a neat diagram. **(10 Marks)**

b. What is the difference between stream cipher and block cipher? **(04 Marks)**

c. Explain the AES key expansion algorithm. **(06 Marks)**

Module-3

5 a. Define and list the axioms of Rings and Fields. **(06 Marks)**

b. State and prove Eulers theorem. **(06 Marks)**

c. Construct an addition and multiplication table for GF(7) and find the values for additive and multiplicative inverse. **(08 Marks)**

OR

6 a. State and prove Fermat's Theorem and calculate $30^{2020} \bmod 19$ using the theorem. **(10 Marks)**

b. Calculate the totient function for
(i) $\phi(240)$ (ii) $\phi(14)$ **(06 Marks)**

c. Define and list the axioms of Groups. **(04 Marks)**

Module-4

7 a. Explain how Diffie Hellman key exchange algorithm is used to exchange secret keys. **(10 Marks)**

b. Consider the elliptic curve $E_{23}(1, 1)$, P = (3, 10) and Q = (9, 7).
Find (i) P + Q (ii) 2P **(10 Marks)**

OR

8 a. Perform encryption and decryption using RSA algorithm for P = 7, Q = 11, e = 13 and M = 5. **(10 Marks)**

b. Explain the scheme of public key cryptosystem for both authentication and secrecy. List the applications of public key cryptosystem. **(06 Marks)**

c. Briefly describe the ways of attaching RSA algorithm. **(04 Marks)**

Module-5

9 a. Explain linear feedback shift register with necessary diagrams and example. **(10 Marks)**

b. Explain the stream ciphers generalized Geffe generator, Threshold generator and Jennings generator with neat diagram. **(10 Marks)**

OR

10 a. Write a note on :
(i) A5
(ii) Hughes XPD/KPD
(iii) Rambutan **(10 Marks)**

b. Elaborate Beth Piper stop and go generator, Alternating stop and go generator and Bilateral stop and go generator of stream ciphers using LFSR's. **(10 Marks)**

* * * * *