CBCS SCHEME

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

21EC642

Sixth Semester B.E./B.Tech. Degree Examination, June/July 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. State the properties of modular arithmetic for integers in Z_n. **(04 Marks)**

b. Explain Euclidean algorithm and apply the algorithm to determine gcd (24140, 16762). **(08 Marks)**

c. Explain Groups, Rings and Fields. **(08 Marks)**

OR

2 a. Prove the following and give an example:
$[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$ **(04 Marks)**

b. For polynomial arithmetic over GF(2) perform addition, multiplication and division for the given polynomials $f(x) = x^4 + x^2 + x + 1$ and $g(x) = x^3 + x^2 + 1$ **(06 Marks)**

c. Apply extended Euclidean algorithm to determine the multiplicative inverse of $(x^7 + x + 1)$ mod $(x^8 + x^4 + x^3 + x + 1)$. **(10 Marks)**

Module-2

3 a. With a neat diagram, explain the model of symmetric cryptosystem. Also explain the independent dimensions along which the cryptographic systems are characterized. **(08 Marks)**

b. Explain the rules of playfair cipher. Using the keyword 'GRADUATE' create play fair matrix and obtain the cipher text for the plaintext 'engineering'. **(08 Marks)**

c. Use Caesar cipher with a key 10 to encrypt the message 'good work'. **(04 Marks)**

OR

4 a. List the briefly explain the different type of cryptanalytic attacks based on what is known to the attacker. **(06 Marks)**

b. Define : i) Unconditionally secure ii) Computationally secure. **(04 Marks)**

c. Encrypt the plaintext "bright" using Hillcipher with the key $K = \begin{bmatrix} 7 & 5 \\ 8 & 3 \end{bmatrix}$. Also show the corresponding calculations to decrypt the message. **(10 Marks)**

Module-3

5 a. Explain the fiestal cipher structure for encryption and decryption. **(06 Marks)**

b. Apply mix column transformation for the following sequence of input bytes "67 78 89 9A". **(08 Marks)**

c. State and prove Fermat's theorem. Also find 3^{201} mod 11 using it. **(06 Marks)**

OR

6 a. Explain the overall scheme of DES encryption algorithm with a neat block diagram. **(08 Marks)**

b. Explain AES key expansion algorithm. **(07 Marks)**

c. Define Euler's totient function. Find Euler's totient function of i) ϕ (41) ii) ϕ (440) iii) ϕ (231) iv) ϕ (27) **(05 Marks)**

Module-4

7 a. With a neat diagram, explain public key cryptosystem to achieve both authentication and secrecy. **(06 Marks)**

b. Explain RSA encryption and decryption algorithm. In public key system using RSA, you intercept the ciphertext c = 10 sent to a user whose public key is c = 5, n = 35. What is the plaintext M? **(08 Marks)**

c. Explain elliptic curve encryption/decryption. **(06 Marks)**

OR

8 a. Users A and B use the Diffie Hellman key exchange mechanism with a common prime Q = 11 and a primitive root $\alpha = 2$. If A selects private key $X_A = 6$ and B selects private key $X_B = 8$, then what is the public key y_A of A and public key y_B. Also what is the secret key shared with A. **(06 Marks)**

b. Explain the man-in-the-middle attack. **(08 Marks)**

c. Which are the possible five approaches to attack RSA algorithm? **(06 Marks)**

Module-5

9 a. Explain linear feedback shift register with necessary diagram. Also explain Galois LFSR. **(08 Marks)**

b. Explain the following with neat diagram:
i) Geffe generator
ii) Alternating stop and go generator
iii) Multispeed inner-product generator. **(12 Marks)**

OR

10 a. Explain Fish and Pike additive generators. **(10 Marks)**

b. Explain : i) Gifford ii) PKZIP. **(10 Marks)**

* * * * *