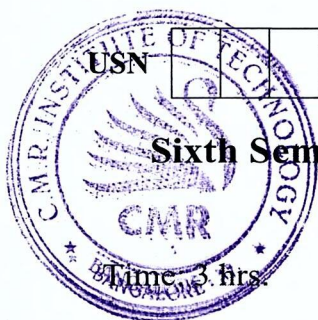


CBCS SCHEME

21EC642



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

Cryptography

Max. Marks: 100

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

Module-1

- 1 a. Explain the Euclidean Algorithm for determining the GCD of two positive integers. Calculate the GCD of 1160718174 and 316258250, using Extended Euclidean algorithm. (10 Marks)
- b. Outline the properties of modular arithmetic. (05 Marks)
- c. Define Divisibility and list the properties of divisibility for integers. (05 Marks)

OR

- 2 a. Develop for an GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operators. Also find the values for additive inverse and multiplicative inverse. (10 Marks)
- b. Discuss the properties of rings, groups and fields. (05 Marks)
- c. List and define the three classes of polynomial arithmetic. (05 Marks)

Module-2

- 3 a. Draw and explain the model of symmetric cryptosystem. (10 Marks)
- b. Encrypt the plaintext "ELECTRONICS" using a Playfair Cipher with key "INDIA", also give the rules for encryption. (10 Marks)

OR

- 4 a. Define transposition and explain the different transposition techniques used in security. (10 Marks)
- b. Using Hill Cipher technique, encrypt and decrypt the plaintext "ATTACK" using the key,
$$\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$
 (10 Marks)

Module-3

- 5 a. Draw a neat block diagram, to explain AES encryption and decryption techniques. (08 Marks)
- b. Illustrate with a neat diagram, Fiestal encryption and decryption model. (08 Marks)
- c. State and prove Euler's theorem. (04 Marks)

OR

- 6 a. Briefly describe the SubBytes and shift Rones in AES algorithm. (08 Marks)
- b. Write and explain with a neat diagram, about DES encryption algorithm. (08 Marks)
- c. State and prove Fermat's Theorem. (04 Marks)

Module-4

- 7 a. Demonstrate with a neat diagram, the public key cryptosystem for authentication. List the requirements for public key cryptography. (10 Marks)
- b. Solve, assuming $p = 17$ and $q = 11$, find public key and private keys. Perform encryption and decryption for plaintext message block $M = 88$ using RSA Algorithm. Consider $e = 7$. (10 Marks)

OR

- 8 a. Explain Diffie-Hellman key exchange algorithm. Show that the keys generated at sender side and receiver side are same. (10 Marks)
- b. Describe the Elliptic curve cryptography. (10 Marks)

Module-5

- 9 a. Develop linear feedback shift registers with necessary diagrams and explain how shift register sequences are used in cryptography. (10 Marks)
- b. Write about linear congruential generators. (05 Marks)
- c. Explain Gifford Algorithm. (05 Marks)

OR

- 10 a. Illustrate the design and analysis of stream Cipher. (10 Marks)
- b. Write with neat diagram about Beth-Piper Stop-and-Go Generator. (05 Marks)
- c. Explain self-decimated generators. (05 Marks)

* * * * *