CBCS SCHEME

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

21EC642

Sixth Semester B.E./B.Tech. 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. Explain Euclidean algorithm to find the GCD of two numbers with the help of an example where a = 234, b = 42. **(10 Marks)**

b. What is modulus and congruent modulo n. State the properties of congruences with the help of an example for each. **(10 Marks)**

OR

2 a. Explain division algorithm with the help of number line. And also state the properties of disability for integers. **(10 Marks)**

b. Explain the procedure used for finding the multiplicative inverse in GF(P) perform arithmetic operations in FG(7). **(10 Marks)**

Module-2

3 a. With the help of neat block diagram, explain the model for network security. **(10 Marks)**

b. Explain the procedure involved in encrypting a massage using play-fair cipher. A message to be sent at an wireless station in play-fair cipher is "cryptography" using the key "MONARCHY" encrypt the message. **(10 Marks)**

OR

4 a. Explain the procedure involved in encrypting a message using hill cipher for m = 3 encrypt the message "herbre" using the hill cipher with the key $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$. Find whether decryption is possible or not. Show your calculations and result. **(10 Marks)**

b. Explain passive and active attacks in network security. **(10 Marks)**

Module-3

5 a. With the help of neat block diagram, explain the salient features of DES encryption algorithm. **(10 Marks)**

b. Explain Euler's theorem with example as a = 2, n = 11. **(10 Marks)**

OR

6 a. Given the plaintext {0 0 0 1 0 2 0 3 0 4 0 5 0 6 0 7 0 8 0 9 0 A 0 B 0 C 0 D 0 E 0 F} and the key {0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 }

i) Show the original contents of state, displayed as a 4 × 4 matrix
ii) Show the value of state after initial Addround key
iii) Show the value of state after shift rows

Make use of AES algorithm. **(10 Marks)**

b. Explain the choice of the parameters used in the design of traditional block cipher/Feistel cipher. **(10 Marks)**

Module-4

7 a. Explain the applications and requirements of public –key cryptosystems. **(10 Marks)**

b. Assuming p = 7 and q = 17, find the public key and private key. Perform encryption and decryption for plain text message block M = 6. **(10 Marks)**

OR

8 a. Show that in Diffie – Hellman key exchange algorithm, the keys generated at sender side and receiver side are same. Assuming q = 23 and α = 5, users A and B select their private keys $X_A = 6$ and $X_B = 15$ compute their public key Y_A and Y_B and shared secret key K. **(10 Marks)**

b. Describe the Elliptic curve cryptography. **(10 Marks)**

Module-5

9 a. Explain LFSR and how the shift register sequences are used in cryptography. **(10 Marks)**

b. Write a note on design and analysis of stream cipher. **(10 Marks)**

OR

10 a. With a neat diagram, explain generalized Geffe generator. **(10 Marks)**

b. Write short notes on :

i) A5 to encrypt GSM

ii) NANOTEQ and RAMBUTAN. **(10 Marks)**

* * * * *