CBCS SCHEME

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

18EC744

Seventh Semester B.E. Degree Examination, June/July 2024
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 various types of attacks on encrypted messages. **(08 Marks)**

b. List the rules of playfair cipher and encrypt the message "Cryptosystem" with the key "MATRIX". **(08 Marks)**

c. Find the GCD of (24146, 16762) using Euclidean algorithm. **(04 Marks)**

OR

2 a. Explain the functionality of symmetric cryptosystem model with a neat diagram. **(08 Marks)**

b. Determine the inverse mod 26 matrix of

i) $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$ ii) $\begin{pmatrix} 1 & 7 & 22 \\ 4 & 9 & 2 \\ 1 & 2 & 5 \end{pmatrix}$

(12 Marks)

Module-2

3 a. Explain the Feistel Cipher structure with the help of a neat diagram. **(10 Marks)**

b. Explain AES key expansion process with a neat diagram and algorithm. **(10 Marks)**

OR

4 a. Explain the AES encryption one round operation with a neat diagram. **(10 Marks)**

b. Explain the DES encryption algorithm structure with a neat diagram. **(10 Marks)**

Module-3

5 a. Find discrete logarithms for the set {1, 2,.....12} with the base 6 modulo 13. **(12 Marks)**

b. Find the multiplicative inverse in GF (ϕ = 1997) of the following: i) 543 ii) 894. **(08 Marks)**

OR

6 a. State the properties that are to be satisfied by a set S, to become a field. **(12 Marks)**

b. It can be shown that if gcd(m, n) = 1 then $\phi(m, n) = \phi(m)\phi(n)$. Also, if P is a prime then $\phi(p) = (p - 1)$, determine number of relatively prime numbers in i) ϕ (26100) ii) ϕ (27783). **(08 Marks)**

Module-4

7 a. Explain the encryption and decryption process of RSA algorithm. Also encrypt the message M = 5 such that p = 11, q = 19 and e = 13. **(12 Marks)**

b. Explain the encryption and decryption process of Elliptic curve cryptography. **(08 Marks)**

OR

8 a. In the elliptic curve group $E_{23}(1, 1)$, consider the points P = (3, 10) and Q = (9, 7). Find the points 2P and P + Q. **(12 Marks)**

b. Explain the Diffie-Hellman key exchange algorithm. Also find the shared key for q = 199, $\alpha = 7$, $X_A = 8$ and $X_B = 13$. **(08 Marks)**

Module-5

9 a. Explain the operation of LFSR in brief. Using a 4-bit LFSR tapped at the 1st and 4th bit, and with initial condition 1111, generate the output sequence. Determine after how many iterations the sequence repeats. **(10 Marks)**

b. Explain the operation of the following generators :

i) Beth-Piper stop-and-go generator

ii) Alternate stop-and-go generator. **(10 Marks)**

OR

10 a. Explain the operation of Gifford generator with a neat diagram. **(08 Marks)**

b. Explain the operation of the following generators

i) Fish generator

ii) Algorithm M. **(12 Marks)**

* * * * *