CBCS SCHEME

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

15EC744

Seventh Semester B.E. Degree Examination, Dec.2023/Jan.2024
Cryptography

Time: 3 hrs. Max. Marks: 80

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

Module-1

1 a. Briefly define a Ring. **(08 Marks)**

b. Explain Euclid's algorithm for determining GCD of two positive integers. Apply Euclid's algorithm to find the GCD (24140, 16762). **(08 Marks)**

OR

2 a. In GF(2^8) find the multiplicative inverse of x^5 modulo $x^8 + x^4 + x^3 + x + 1$ using extended Euclidean algorithm. **(08 Marks)**

b. Consider the following polynomials in GF(2^8) :
$f(x) = x^6 + x^4 + x^2 + x + 1$, $g(x) = x^7 + x + 1$, $m(x) = x^8 + x^4 + x^3 + x + 1$. Find $f(x) * g(x)$ mod $m(x)$ using binary arithmetic. **(08 Marks)**

Module-2

3 a. List and briefly define types of cryptanalytic attacks based on what is known to the attacker. **(06 Marks)**

b. Define: Brute force attack and computationally secure encryption. **(04 Marks)**

c. Encrypt the message "punctual and attentive" using playfair cipher with a key "OCCURRENCE". **(06 Marks)**

OR

4 a. Encrypt the message "secure" using hill cipher with the key $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ and also compute K^{-1} required for decryption. **(10 Marks)**

b. Explain the overall scheme of DES encryption with a neat diagram. **(06 Marks)**

Module-3

5 a. Briefly describe mix column transformation. Compute the output of mix column transformation for the following sequence of input bytes "67 89 AB CD". **(08 Marks)**

b. Explain the AES key expansion algorithm. **(08 Marks)**

OR

6 a. Explain the Galois configuration of LFSR. Write a C code for the same. **(08 Marks)**

b. Explain the following LFSR based keystream generators:
i) Jennings generator
ii) Alternating stop and go generator. **(08 Marks)**

Module-4

7 a. State and prove Euler's theorem. (06 Marks)

b. Explain the Chinese remainder theorem. (06 Marks)

c. Represent 973 mod 1813 as a pair of numbers mod 37 and 49. (04 Marks)

OR

8 a. Explain RSA algorithm. Perform encryption and decryption using RSA algorithm for $p = 7$, $q = 11$, $e = 17$ and $M = 8$. (10 Marks)

b. Users A and B use the Diffie Hellman key exchange technique with a common prime $q = 71$ and a primitive root $\alpha = 7$.

i) If user A has private key $X_A = 5$, what is A's public key Y_A?

ii) If user B has private key $X_B = 12$, what is B's public key Y_B?

iii) What is the shared secret key? (06 Marks)

Module-5

9 a. Explain the MD5 algorithm with neat diagrams. (08 Marks)

b. Describe Secure Hash Algorithm (SHA) and discuss its security. (08 Marks)

OR

10 a. Describe the Digital Signature Algorithm (DSA). (08 Marks)

b. Explain :

i) One way Hash function MAC

ii) Stream cipher MAC. (08 Marks)

* * * * *