CBCS SCHEME

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

15EC744

Seventh Semester B.E. Degree Examination, June/July 2023
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 the following: (i) Group (ii) Ring (iii) Field **(06 Marks)**

b. Define Euclidean algorithm. Find the gcd(1160718174, 316258250) by Euclidean algorithm. **(10 Marks)**

OR

2 a. List three classes of polynomial arithmetic. **(02 Marks)**

b. Determine which of the following are reducible over GF(2).
(i) $x^4 + 1$ (ii) $x^3 + x + 1$ **(04 Marks)**

c. Find the gcd(1759, 550) and also calculate x and y using extended Euclidean algorithm and also determine the gcd[a(x), b(x)] for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^4 + x^2 + x + 1$ **(10 Marks)**

Module-2

3 a. With neat diagram, explain simplified model of symmetric encryption. **(08 Marks)**

b. What is hill cipher? Decrypt the cipher text "CQSUBJNR" using Hill Cipher technique with the key = $\begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$ **(08 Marks)**

OR

4 a. With neat diagram, explain DES encryption and decryption process. **(08 Marks)**

b. Explain play fair cipher with rules. Encrypt the plaintext "have his car case" using play fair cipher with the key "Monday". **(08 Marks)**

Module-3

5 a. With neat diagram, explain AES encryption and decryption. **(10 Marks)**

b. What is linear feedback shift register? And also explain 4-bit LFSR. **(06 Marks)**

OR

6 a. Write notes on:
(i) Shift row transformation
(ii) Mix column transformation **(08 Marks)**

b. How to design stream ciphers wing LFSR's and discuss the following with diagrams:
(i) Gaffe generator
(ii) Beth-piper stop and go generator **(08 Marks)**

Module-4

7 a. State and prove the Fermat's theorem with example. **(08 Marks)**

b. Briefly explain Diffie-Hellman key exchange. **(08 Marks)**

OR

8 a. What is Euler's totient function? **(02 Marks)**

b. Determine the Euler totient function for the following:
(i) $\phi(41)$ (ii) $\phi(37)$ (iii) $\phi(10)$ **(06 Marks)**

c. User A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and 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 secrete key? **(08 Marks)**

Module-5

9 a. What is hash function? What is the method that has been proposed to generate a longer hash value than a given hash function produces? **(08 Marks)**

b. What is digital signature algorithm? Explain the description of DSA. **(08 Marks)**

OR

10 a. Write short notes on:
(i) SNEFRU
(ii) MD4 **(08 Marks)**

b. Briefly discuss the following:
(i) DSA variants
(ii) GOST digital signature algorithm **(08 Marks)**

* * * * *