CBCS SCHEME

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

17EC744

Seventh Semester B.E. Degree Examination, Jan./Feb. 2021
Cryptography

Time: 3 hrs. Max. Marks: 100

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

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-1

1 a. What is Divisibility? Explain the division algorithm with suitable example. **(06 Marks)**
b. Explain with examples the properties of modular Arithmetic. **(06 Marks)**
c. Write a note on Finite field of the Form GF(P). **(08 Marks)**

OR

2 a. Write the Arithmetic addition modulo and multiplication module for GF (2^4). **(06 Marks)**
b. With suitable example, explain the polynomial Arithmetic with co-efficient in Z_P. **(08 Marks)**
c. What are Groups? Explain in detail with respect to its properties. **(06 Marks)**

Module-2

3 a. With a neat sketch, explain the model of symmetric cryptosystems. **(06 Marks)**
b. For the keyword "ELECTRONICS", Give the cipher text for the plain text "COMMUNICATION ENGINEERING", using play fair cipher. Explain the rules for play fair cipher. **(10 Marks)**
c. Explain with an example, how the transposition technique is used to convert PT to CT. **(04 Marks)**

OR

4 a. What is Stegnography? Explain different methods adopted in stegnography. **(06 Marks)**
b. Explain simplified DES algorithm with a neat block diagram. **(08 Marks)**
c. Explain with suitable sketch, the concept of Feistel encryption and decryption. **(06 Marks)**

Module-3

5 a. List and explain the algorithm and characteristics implementation and AES. **(08 Marks)**
b. Explain the Key-Block-Round combination analysis in AES. **(06 Marks)**
c. Explain the concept of AES encryption single Round stages. **(06 Marks)**

OR

6 a. Explain in detail the nonlinear shift Register. **(06 Marks)**
b. Write an explanatory note on Linear Feed Back Shift Registers. **(10 Marks)**
c. Compare different LFSR boxed stream ciphers for its ryptographical weaknesses. **(04 Marks)**

Module-4

7 a. Find the GCD of (1970, 1066) using Euclid's method. **(04 Marks)**
b. With suitable explanation prove Euler's theorem. **(07 Marks)**
c. Explain Chaises Remainder Theorem and its features. **(09 Marks)**

OR

8 a. Explain the complete steps involved for encryption key Generation and Decryption for RSA algorithm. **(08 Marks)**

b. What is Key Management? Explain DH key exchange mechanism. **(08 Marks)**

c. Users A and B use the DH key exchange technique. A common prime Q = 353 and a primitive root $\alpha = 3$, If A select private key $X_A = 97$ and B selects private key $X_B = 233$, then, what is public key Y_A of A and public key Y_B. Calculate shared secret key 'K'. **(04 Marks)**

Module-5

9 a. What are one way Hash Functions? Explain in detail one way hash function using symmetric block algorithms. **(08 Marks)**

b. Write an explanatory note on MAC. **(06 Marks)**

c. Briefly explain the security threats on Hash function and MAC. **(06 Marks)**

OR

10 a. Explain in detail Direct Digital Signature and Arbitrated Digital Signature. **(08 Marks)**

b. Explain with suitable sketch, Discrete Logarithm signature scheme. **(06 Marks)**

c. Briefly, explain the signing and verifying the Digital Signature Algorithm (DSA). **(06 Marks)**

* * * * *