CBCS SCHEME

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

18EC744

Seventh Semester B.E. Degree Examination, July/August 2022
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. Describe the simplified model of Symmetric encryption scheme and its ingredients. **(15 Marks)**

b. Explain Euclidean algorithm to find the GCD of two integers. **(05 Marks)**

OR

2 a. With suitable example, explain the Substitution Cipher. **(08 Marks)**

b. Explain the Transposition Cipher. **(07 Marks)**

c. Write the properties of Modular Arithmetic. **(05 Marks)**

Module-2

3 a. Describe the overall scheme for DES algorithm and its salient features. **(15 Marks)**

b. What are the strengths of DES algorithm? **(05 Marks)**

OR

4 a. Present an overview of the general structure of Advanced Encryption standard. **(10 Marks)**

b. Describe the AES key expansion algorithm. **(10 Marks)**

Module-3

5 a. Distinguish between Groups , Rings and Fields. **(12 Marks)**

b. Define Discrete Logarithms with an example. **(08 Marks)**

OR

6 a. With examples, describe Fermats and Eulers theorem. **(12 Marks)**

b. Define the fields of the form GF(P). **(08 Marks)**

Module-4

7 a. Present an overview of the RSA algorithm. **(10 Marks)**

b. Describe Elliptic Curve Cryptography. **(10 Marks)**

OR

8 a. Describe Diffie – Hellman key exchange algorithm. **(10 Marks)**

b. What are the basic principles of Public key Cryptography? **(05 Marks)**

c. What are the possible approaches to attack the RSA algorithms? **(05 Marks)**

Module-5

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

b. Write note on : Design and Analysis of Stream Cipher. **(10 Marks)**

OR

10 Write short note on :

a. Geffe generator. **(06 Marks)**

b. A5 to encrypt GSM. **(06 Marks)**

c. NANOTEQ and RAMBUTAN. **(08 Marks)**

* * * * *

CMRIT LIBRARY
BANGALORE - 560 037