Roll No. ......................

Total Page No. : 2

610403/
610903

# 610403/610903

# B.TECH. VI SEM MAIN/BACK EXAM
# AUGUST 2023

# COMPUTER SCIENCE AND ENGINEERING

# (6CS4-03) - INFORMATION SECURITY SYSTEM

# COMMON WITH CSE & IT

**Time :** 3 Hours]

[**Max. Marks :** 80

[**Min Passing Marks :**

**Instructions to Candidates :** Part – A: Short answer questions (up to 25 words) 5 × 2 marks = 10 marks. All 5 questions are compulsory.

Part – B: Analytical Problem Solving questions 4 × 10 marks = 40 marks. Candidates have to answer 4 questions out of 6.

Part – C: Descriptive Analytical Problem Solving questions 2 × 15 marks = 30 marks. Candidates have to answer 2 questions out of 3.

Schematic diagrams must be shown wherever necessary. Any data you feel missing may suitably be assumed and stated clearly. Units of quantities used/calculated must be stated clearly.

Use of following supporting materials is permitted during examination. (Mentioned in form No. 205)

**1 : Nil** **2 : Nil**

## PART A

1. Explain the three security principles.

2. What do you understand by Risk, Vulnerability and Threat in a network ?

3. How is Encryption different from Hashing ?

4. What is the difference between stream cipher and block cipher ?

5. List down different modes of operation.

## PART B

1. Explain transposition cipher with example.

2. Explain the single round of the DES algorithm with a neat block diagram. What is the purpose of s-boxes in DES ?

3. Describe the Chinese remainder theorem with an example.

4. What is the Primitive Root ? Explain an algorithm to determine Primitive roots. Determine all the Primitive roots of 19.

5. What is an SSL Certificate and how does it Work ? What so SSL certificates do for websites ?

6. What is public key cryptography ? What are the principle in gredients of a public-key cryptosystem ?

## PART C

1. What is a primitive root ? Explain the Diffie-Hellman key exchange algorithm with a proper example. Discuss the man-in-the-middle attack problem associated with the algorithm.

2. Explain the RSA algorithm. In an RSA system, it is given that p = 11, q = 13, e = 7 and M = 5. Find ciphertext C and M from decryption.

3. What is Digital Signature ? List the security services provided by digital signature. Explain its uses with the help of an example.