Roll No. □□□□□□□□□□□□ Total No. of Pages : 02

Total No. of Questions : 09

B.Tech. (CSE) (Sem.–7,8)

NETWORK SECURITY AND CRYPTOGRAPHY

Subject Code : BTCS701-18

M.Code : 90487

Date of Examination : 12-12-2022

Time : 3 Hrs. Max. Marks : 60

INSTRUCTIONS TO CANDIDATES :

1. SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.
2. SECTION-B contains FIVE questions carrying FIVE marks each and students have to attempt any FOUR questions.
3. SECTION-C contains THREE questions carrying TEN marks each and students have to attempt any TWO questions.

SECTION-A

1. **Write briefly :**

   a) What is Vulnerability?

   b) What is modular arithmetic give an example to explain?

   c) What is the importance of prime numbers in cryptography?

   d) AES.

   e) What does CIA model?

   f) Define threat and attack.

   g) Euler's Theorem.

   h) Kerberos.

   i) PGP.

   j) Block cipher.

SECTION-B

2. Differentiate Active and Passive attack.

3. What is Conventional Encryption Model? Explain.

4. Explain the different mode of operations.

5. Give details of RSA algorithm with the help of suitable example.

6. Explain any two key distribution techniques.

SECTION-C

7. Explain the followings:

   a) IDS

   b) Email Security.

8. What are the main Threats in networks .Explain the network Security Control Archicture.

9. Give details of the following :

   a) Secure Hash Algorithm

   b) Digital signature.