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

Total No. of Questions : 09

B.Tech. (Computer Science & Engg.)(Sem.–7,8)

NETWORK SECURITY AND CRYPTOGRAPHY

Subject Code :BTCS-701-18

M.Code : 90487

Date of Examination : 01-07-22

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 cryptography?

b) What is modular arithmetic. Give an example to explain?

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

d) Differentiate between authorization and authentication.

e) What does CIA stands for?

f) Define threat and attack.

g) Hash Function

h) PFP

i) IDS

j) Block cipher

SECTION-B

2. Explain the Euclidean and Extended Euclidean algorithm.

3. Differentiate Active and Passive attack.

4. What is the purpose of S-boxes in DES?

5. Identify the possible threats for RSA algorithm and list their counter measures.

6. What are the types of attack on encrypted message. Explain.

SECTION-C

7. Explain the following :

   a) MD5 message Digest Algorithm.

   b) Digital Signature.

8. Explain the design and types of firewalls.

9. Perform encryption and decryption using RSA algorithm for the following :

   P=7; q= 11; e=17; M=8.

NOTE : Disclosure of Identity by writing Mobile No. or Making of passing request on any page of Answer Sheet will lead to UMC against the Student.