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

Total No. of Questions : 09

B.Tech. (CSE) (Sem.–7)

NETWORK SECURITY AND CRYPTOGRAPHY

Subject Code : BTCS-701-18

M.Code : 90487

Date of Examination : 17-05-23

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 analysis?

b. Give example of few active threats.

c. What is non-repudiation?

d. State Fermat theorem.

e. Why SHA is more secure than a hash function?

f. What is the difference between firewall and antivirus?

g. What is Kerberos?

h. What are digital signatures?

i. Why do we use captchas?

j. What is port scan attack?

SECTION-B

2. Explain various active threats with the help of an example.

3. What is a block cipher? Discuss block ciphers modes of operations.

4. Discuss the different requirements for message authentication.

5. Why do we need digital signatures? How digital signature works?

6. How do honeypots work? Discuss the placement of honeypots in a network.

SECTION-C

7. Describe the steps in finding the message digest using SHA-512 algorithm. What is the order of finding two messages having the same message digest?

8. Explain the working of RSA algorithm with the help of a suitable example. Mention any one technique attacking RSA.

9. Write a short note on :

   a. Key distribution techniques

   b. Purpose of S-box in DES.

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.