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: 05-01-2026

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 the concept of block ciphers?

b) Give the header format of ESP in IPSec.

c) How the nonlinearity is achieved in DES.

d) How digital signature is implemented using RSA approach?

e) Explain the mix column operation in AES algorithm.

f) What is distributed denial service attack?

g) What are the threats in networks?

h) What are the requirements of a good hash function?

i) Differentiate between Euclidian and extended Euclidian algorithm.

j) List the various attacks that can be made on packet filtering routers and mention appropriate countermeasures.

SECTION - B

2. You are required to implement secure web access in your organization. Which protocol will you use for the purpose? Explain secure connection establishment ant protocol to encrypt messages in details with suitable diagrams.

3. Explain briefly the MD5 algorithm. How it is different from earlier versions of it?

4. Illustrate man in the middle attack on Diffie Hellman key exchange algorithm.

5. Explain the concept of wireless security. List its various protocols available. Identify and mitigate software security vulnerabilities in existing systems.

6. Differentiate between monoalphabetic and polyalphabetic ciphers with example.

SECTION - C

7. Explain Elgamal encryption system for Public-Key cryptography. Why this system is able to thwart man-in the middle attack? Give mathematical proof of this algorithm.

8. **Write a short note with the help of suitable example:**

   a. Kerberos

   b. Honeypots

   c. IDS

   d. Personal Firewalls

9. What is Rivest, Shamir, Adleman algorithm? Give mathematical proof of this algorithm. Explain with the help of suitable example. Use suitable assumption, if any.

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.