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 : 28-04-2025

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) Security Threat

b) Passive Attack

c) Mod of an expression.

d) Cryptography

e) Access control

f) Need of Wireless Security.

g) Honeypot

h) Purpose of Firewall.

i) Message Authentication code

j) Content Integrity

SECTION - B

2. How conventional Encryption model works? Explain in detail.

3. Write a note on modular arithmetic.

4. Explain in detail principles of public-key cryptography.

5. How MD5 Message Digest Algorithm Works? Explain in detail.

6. Explain in detail design and Types of Firewalls.

SECTION - C

7. Explain in detail about Fermat and Euler's Theorem.

8. Write a short note on Elliptic Curve Cryptography.

9. Compare RSA Algorithm with AES Algorithm on different parameters. Explain their used cases also.

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.