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 : 29-12-2023

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 modular arithmetic, and how does it relate to encryption algorithms?

b) Differentiate between symmetric and asymmetric encryption algorithms.

c) What role do substitution and transposition techniques play in classical cryptography?

d) How does a Message Authentication Code (MAC) ensure the integrity of a message?

e) What is the fundamental role of encryption in network security?

f) Define a prime number and its significance in cryptography.

g) Name a common cryptographic algorithm used for symmetric encryption.

h) Differentiate between a MAC (Message Authentication Code) and a digital signature.

i) What does SSL/TLS stand for, and what is its function in secure communication?

j) Define a firewall and its role in network security.

SECTION-B

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

3. Define the properties of a secure hash function in detail and discuss the importance of collision resistance, preimage resistance and second preimage resistance in maintaining data integrity and authenticity.

4. Compare and contrast cryptographic hash functions and MAC (Message Authentication Code) algorithms, outlining their purposes, construction principles, and use cases.

5. Analyze the security implications of length extension attacks on hash functions, detailing how these attacks can compromise the integrity of hashed data.

6. Describe the role of hashing and asymmetric encryption in the generation of a digital signature.

SECTION-C

7. Describe the steps involved in generating RSA key pairs. How does the length of the key affect the security of the encryption?

8. Discuss the challenges and considerations in designing a secure wireless network, covering topics such as authentication protocols, encryption mechanisms and protection against attacks like eavesdropping and jamming.

9. Describe the role of a Virtual Private Network (VPN) in securing communication over public networks, examining its architecture, tunnelling protocols and encryption techniques.

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.