

B.Sc. Sem.-6 (Rep) Examination

SE-311

Computer Science (B)

(CIS)

Time : 2-30 Hours]

October-2025

[Max. Marks : 70

- Q.1 (A) Define **Network Security**. Explain the **principles, goals, and importance** of network security in modern communication systems. 7
- (B) Describe the **CIA Triad (Confidentiality, Integrity, Availability)** with examples. How do these properties ensure secure communication? 7
- OR
- (A) What are **security services and mechanisms**? Explain the relationship between them using the **OSI Security Architecture**.
- (B) Discuss the **various threats** to network security and their preventive measures.
- Q.2 (A) Explain the Advanced Encryption Standard (AES) algorithm. How is it different from DES? 7
- (B) What is Key Distribution? Explain various methods of key distribution in conventional encryption systems. 7
- OR
- (A) Define Symmetric Cipher. Explain its working principle with a neat diagram.
- (B) Explain the Data Encryption Standard (DES) algorithm in detail.
- Q.3 (A) Define Web Security. Explain the need and importance of Web Security in modern Internet applications. 7
- (B) Explain the various types of Web Security threats and their countermeasures. 7
- OR
- (A) Explain various threats and attacks on databases. How can database security be ensured?
- (B) Discuss the major security issues in wireless networks and explain possible solutions.
- Q.4 (A) Explain the major security issues in E-Commerce and M-Commerce and discuss their solutions. 7
- (B) Explain the concept of Web Encryption using SSL/TLS protocols. 7
- OR
- (A) Explain Session Hijacking and Session Fixation attacks with prevention methods.
- (B) Describe Digital Certificates and the role of Certificate Authorities (CA) in Web Security.
- Q.5 MCQ 14
- 1. Which of the following is a primary goal of Information Security?**
- A. Confidentiality, Integrity, Availability
- B. Encryption, Authentication, Authorization
- C. Firewalls, Antivirus, Backup
- D. None of the above

P.T.O

N 720.2

2. What does "Confidentiality" ensure in information security?

- A. Data is available when needed
- B. Data is not altered
- C. Data is accessible only to authorized users
- D. Data is encrypted

3. Which of the following is an example of a security attack?

- A. Encryption
- B. Authentication
- C. Phishing
- D. Backup

4. What is the process of converting plain text into unreadable form called?

- A. Decryption
- B. Cryptography
- C. Encryption
- D. Encoding

5. Which of the following is not a type of malware?

- A. Virus
- B. Worm
- C. Firewall
- D. Trojan horse

6. Which of the following ensures that data has not been altered during transmission?

- A. Confidentiality
- B. Integrity
- C. Availability
- D. Authentication

7. The process of verifying the identity of a user is called:

- A. Authorization
- B. Authentication
- C. Accounting
- D. Access Control

→ X ←