2/21

0305N215

Candidate's Seat No :_____

MSc Sem.-2 Examination

409

Computer Science

Time : 2-30 Hours] **May-2025** **[Max. Marks : 70**

Q:1 (A) Explain the difference between computer security and information security. Why is information security crucial for organizations? (7)

Q:1 (B) What are firewalls? Discuss the different types of firewalls and their limitations in network security. (7)

OR

Q:1 (A) What is Intrusion Detection and Prevention? Discuss the types and limitations of IDS/IPS systems. (7)

Q:1 (B) What is Steganography? How is it used for securing communication? Discuss the role of classical encryption techniques in modern cryptography. (7)

Q:2 (A) Explain the process of data encryption using classical ciphers such as Caesar Cipher, Vigenère Cipher, and Playfair Cipher. (7)

Q:2 (B) Explain the web security threats and attacks that can compromise a website's integrity and security. Discuss common database security threats. How can these threats be mitigated? (7)

OR

Q:2 (A) Explain the working of block ciphers. How do they differ from stream ciphers? Describe the DES (Data Encryption Standard) algorithm. What are its strengths and weaknesses? (7)

Q:2 (B) What are Triple DES and AES? How do they improve upon DES in terms of security? (7)

Q:3 (A) Compare and contrast modern symmetric ciphers like AES and older ciphers like DES. (7)

Q:3 (B) Discuss the application of symmetric ciphers in real-world systems. How are they implemented in modern encryption systems? (7)

OR

(P.T.O)

N215-2

Q:3 (A) How does the security of conventional encryption compare to modern symmetric encryption algorithms? (7)

Q:3 (B) What is malicious logic in information security? Explain the different types of malicious software (malware). (7)

Q:4 (A) What are countermeasures in information security? Provide examples of both preventative and reactive countermeasures. (7)

Q:4 (B) Discuss the significance of confidentiality and integrity policies in an organization. How do these policies contribute to overall security? (7)

OR

Q:4 (A) Explain the concept of security incidents and attacks. Discuss common network security incidents. (7)

Q:4 (B) Describe the role of boundary devices in network security. How do they protect an organization's network? (7)

Q:5 True/False Attempt any seven out of Twelve (Each carries 2 Marks) (14)

1 Information security only deals with protecting physical assets like computers and servers.

2 A threat is any circumstance or event that has the potential to harm an information system, such as unauthorized access or malware.

3 Malicious logic refers to harmful programs like viruses and worms, which can compromise the confidentiality, integrity, and availability of data.

4 Network security incidents can only occur from external attackers, not internal users.

5 Boundary devices like routers and firewalls are used to monitor and control traffic between different networks, providing a layer of security.

6 Firewalls are limited to only blocking incoming network traffic; they cannot block outgoing traffic.

7 Web threats and attacks include SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

8 Database security only focuses on encryption of data but does not concern user access control.

9 Wireless networks are more vulnerable to attacks due to weak encryption and open communication channels.

10 The conventional encryption model uses the same key for both encryption and decryption.

11 In block ciphers, plaintext is divided into blocks before encryption.

12 AES (Advanced Encryption Standard) is a symmetric key encryption algorithm that is widely used today.