

SUBJECT:- INFORMATION AND CYBER SECURITY

CLASS:- BCA 6TH SEM

PREPARED BY:- SHIVANSH SIR

1. What is Information Security? Explain its key principles with suitable examples.
2. What is Cyber Security? Discuss its importance and challenges in detail.
3. What is Cryptography? Explain the different types of cryptographic techniques.
4. What is Public Key Infrastructure (PKI)? Explain its components and working mechanism.
5. What is a Firewall? Discuss its types and how it protects a network.
6. What is Malware? Explain different types of malware such as viruses, worms, Trojan horses, and ransomware.
7. What is the difference between Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks? Explain with examples.
8. What are Security Policies and Procedures? Explain the components of an effective security policy.
9. Explain the stages of the Security Risk Management process with examples.
10. What is a Security Audit? Discuss its types and the importance of conducting security audits.
11. Explain Network Security Protocols such as SSL/TLS. How do they ensure secure communication?
12. What is Multi-Layered Defense (Defense in Depth) in Cyber Security? Explain its importance with examples.
13. Discuss the concept of Ethical Hacking. How does it help in strengthening security systems?
14. What are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)? Explain their working mechanisms.
15. What is Social Engineering? Explain different techniques used in social engineering attacks.
16. Discuss the concept of VPN (Virtual Private Network). How does it ensure secure data transmission?
17. What is Two-Factor Authentication (2FA)? How does it enhance system security?
18. What is Data Encryption? Explain symmetric and asymmetric encryption with examples.
19. What is Cyber Forensics? Discuss its importance and the key steps involved in a cyber forensic investigation.
20. What is the difference between Authentication and Authorization? Explain their roles in system security.