Exam. Code: 1000
Sub. Code: 34997

2055

M.E. (Computer Science and Engineering)
Second Semester
Elective - IV
CS-8207: Network Security

Time allowed: 3 Hours Max. Marks: 50

NOTE: Attempt any five questions. All questions carry 10 marks.

x-x-x

1. What is the difference between authentication and authorization in the context of information security, and why is it important to separate the two processes?

2. Explain the difference between a Denial-of-Service (DoS) attack and a Distributed Denial-of-Service (DDoS) attack. How does the distributed nature of a DDoS attack make it more difficult to defend against?

3. In symmetric key cryptography, both the sender and the receiver use the same secret key for encryption and decryption. What are the main challenges in securely sharing and managing this key, especially in large-scale systems?

4. The Data Encryption Standard (DES) uses a 56-bit key and operates on 64-bit blocks of data. Given its structure and key length, discuss the primary vulnerabilities of DES in the context of modern computational capabilities. How do these vulnerabilities affect its suitability for secure communications today?

5. Explain how Diffie-Hellman is achieved without transmitting the secret itself. What are the main security assumptions underlying the protocol, and what types of attacks is it vulnerable to if not properly implemented (e.g., without authentication)?

6. Describe how a digital signature is generated and verified using public key cryptography. What would be the consequences if a private key used for signing is compromised?

P.T.O.

7. Compare and contrast Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in terms of their functionality, deployment, and response to threats. In what scenarios would deploying one over the other—or both together—be most effective?

8. Explain the differences between Network Address Translation (NAT) and Port Address Translation (PAT). How does PAT help in conserving IP addresses, and what impact can it have on applications that require inbound connections?

9. Describe the primary functions of SSL/TLS in ensuring secure data transmission. How do these protocols achieve confidentiality, integrity, and authentication?

x-x-x