Professional Course (Even) Examination, 2025

(6th Semester)

BACHELOR OF COMPUTER APPLICATIONS

(Computer Networking—II)

Full Marks : 75

Time : 3 hours

The figures in the margin indicate full marks for the questions

(PART : A—OBJECTIVE)

(*Marks* : 25)

SECTION—I

(*Marks* : 15)

I. Tick (✓) the correct answer in the brackets provided : 1×10=10

1. What is the primary technique used in a Dictionary Attack?

   (a) Trying every possible combination of characters ( )

   (b) Using a pre-compiled list of common words and phrases ( )

   (c) Intercepting network traffic ( )

   (d) Flooding the server with traffic ( )

2. 'Man-in-the-middle' attack refers to

(a) an attacker intercepting communication between two parties to alter or steal data ( )

(b) an attacker sending malicious e-mails to users ( )

(c) an attacker flooding a server with fake traffic ( )

(d) an attacker inserting malicious code into a website ( )

3. The plaintext is the original message before transformation. The message after transformation is called

(a) encryption ( )

(b) ciphertext ( )

(c) cryptography ( )

(d) decryption ( )

4. Which asymmetric encryption algorithm is widely used for secure communications and is based on the mathematical properties of large prime numbers?

(a) DES ( )

(b) AES ( )

(c) RSA ( )

(d) Diffie-Hellman ( )

5. Which of the following protocols is used to secure communications for web applications by providing encryption and data integrity?

(a) IPsec ( )

(b) SSL/TLS ( )

(c) SSH ( )

(d) ICMP ( )

6. Which of the following is a technique used to verify the identity of a user or system?

(a) Encryption ( )

(b) Authentication ( )

(c) Confidentiality ( )

(d) Hashing ( )

7. In PGP, what is the purpose of the 'key ring'?

(a) To encrypt and decrypt messages securely ( )

(b) To store user credentials for authentication ( )

(c) To generate and exchange cryptographic keys ( )

(d) To store the public and private keys of a user ( )

8. IPsec defines two protocols, which are

(a) AH and ESP ( )

(b) AH and SSL ( )

(c) PGP and ESP ( )

(d) PGP and SSL ( )

9. What is the primary purpose of a port scanner in network security?

(a) To perform vulnerability assessments on the network ( )

(b) To protect the network from incoming attacks ( )

(c) To identify open and closed ports on a target system ( )

(d) To scan for malware on devices in a network ( )

10. Which of the following is not typically performed by malicious virus removers?

(a) Scanning for viruses and malware ( )

(b) Removing harmful files and quarantining them ( )

(c) Preventing unauthorized access to a system ( )

(d) Updating virus definitions for new threats ( )

II. State whether the following are *True (T)* or *False (F)* by putting a Tick (✓) mark in the brackets provided : 1×5=5

1. Spoofing describes an attack where the attacker floods an e-mail system with a large volume of e-mails to overwhelm the recipient.

(T / F)

2. DES uses 16 rounds, while AES uses 10, 12, or 14 rounds depending on the key size.

(T / F)

3. The transport layer of the OSI model is responsible for securing end-to-end communication across the network.

(T / F)

4. Proxy firewalls act as intermediaries between clients and the destination server, forwarding requests and responses.

(T / F)

5. IDPS can only detect attacks but cannot stop them.

(T / F)

SECTION—II

(*Marks* : 10)

III. Answer the following questions : 2×5=10

1. *(a)* How does multifactor authentication contribute to the internetwork security model?

OR

(b) What is the difference between a virus and a worm in the context of cyber attacks?

2. *(a)* What is a digital signature?

OR

(b) Differentiate between Message integrity and Message authentication.

3. *(a)* Write two functions of SHA-1 in network security.

OR

(b) Define MAC and HMAC.

4. *(a)* What is the importance of a certificate in PGP?

OR

(b) What is IP security?

5. *(a)* What is the function of operating system detection tools in network security?

OR

(b) Write a short note on IDPS.

(PART : B—DESCRIPTIVE)

(*Marks* : 50)

IV. Answer the following questions : 10×5=50

1. *(a)* Write short notes on the following : 2×5=10

   (i) Hoaxes

   (ii) Virus

   (iii) Mail bombing

   (iv) Social engineering

   (v) Phishing

OR

(b) Explain the difference between a DoS attack and a DDoS attack. What makes DDoS attacks harder to defend against, and how can we protect against them? 10

2. *(a)* Discuss the differences between Symmetric and Asymmetric key cryptography, highlighting their key characteristics and algorithms. 10

OR

(b) Alice and Bob want to establish a shared secret key using the Diffie-Hellman algorithm. They agree on prime number **p** = 4 and **q** = 3. Alice's private key is **a** = 1, and Bob's private key is **b** = 2. Calculate the shared secret key derived by both parties. Show the steps involved in the process. 10

3. *(a)* Write notes on the following : 5+5=10

   (i) Entity authentication

   (ii) Message digest

OR

(b) Describe the key protocols involved in transport layer security (TLS) and their role in securing communication. 10

4. *(a)* What is a firewall? Explain the Packet-filter firewall and Proxy firewall in detail. 10

OR

(b) Discuss the advantages of using a virtual private network (VPN) for secure communication. 5

(c) What is IKE? How does IKE work in IPsec? 5

5. *(a)* What is antivirus software, and what are its main roles in protecting computers and networks from cyber attacks? 10

OR

(b) Discuss the following security threats and explain the methods to prevent network systems from these attacks : 5+5=10

(i) Worm

(ii) Packer sniffer

★ ★ ★