

2025

(6th Semester)

BACHELOR OF COMPUTER APPLICATIONS

Paper : NIS-602

(Networks and Information Security)

Full Marks : 70

Pass Marks : 45%

Time : 3 hours

(PART : B—DESCRIPTIVE)

(Marks : 45)

*The figures in the margin indicate full marks
for the questions*

1. Explain the need for information security in modern organizations and discuss the key attributes of information security. Provide examples to illustrate your answer. 9

Or

Define threats and vulnerabilities in information security and provide one example of each. List and explain three types of security attacks, highlighting their impacts. 3+6=9

(2)

2. Enumerate and explain the steps involved in the Data Encryption Standard (DES) algorithm. 9

Or

Public key cryptography is a foundational technology in modern secure communications. Answer the following : 2+3+4=9

- (a) Define public key cryptography and explain the concept of a key pair.
- (b) In everyday terms, describe how public key cryptography enables two people who have never met to communicate securely without needing to share a secret key in advance.
- (c) Discuss two practical applications of public key cryptography and explain how each application benefits from using this technology.

3. Explain Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). What roles do they play in network communication? 9

Or

What is IP Security (IPSec) and how does its architecture ensure secure communication over IP networks?

(3)

4. Outline the steps involved in the SSL handshake process between a client and a server. Describe the key cryptographic algorithms utilized in SSL, including their roles in ensuring secure communication. 6+3=9

Or

Describe the operational mechanisms of SMTP and POP3, including the standard ports utilized and the sequence of actions performed during e-mail handling. Evaluate the advantages and limitations of SMTP and POP3. 5+4=9

5. Discuss the fundamental design principles and characteristics of firewalls. In your answer, explain how these principles guide firewall configuration and contribute to an effective network security strategy. 9

Or

Compare and contrast the following firewall technologies : 3×3=9

- (a) Packet Filtering Router
- (b) Stateful Inspection Firewall
- (c) Application-Level Gateway (or Proxy)

2025

(6th Semester)

BACHELOR OF COMPUTER APPLICATIONS

Paper : NIS-602

(Networks and Information Security)

(PART : A—OBJECTIVE)

(Marks : 25)

The figures in the margin indicate full marks for the questions

I. Choose the most appropriate answer and put a Tick (✓) mark against the brackets provided : 1×10=10

1. What is the main difference between a virus and a worm in terms of how they spread?

(a) A virus spreads by attaching itself to programs or files, while a worm spreads on its own without user intervention ()

(b) A worm needs a host file to propagate, whereas a virus spreads independently ()

(c) A virus spreads only through e-mail attachments, while a worm spreads through software downloads ()

(d) A worm requires manual execution by the user, whereas a virus spreads automatically ()

2. What is the primary goal of a Denial-of-Service (DoS) attack?

(a) To steal sensitive data from the target system ()

(b) To interrupt and modify communications between users ()

(c) To overwhelm the target system with excessive traffic, rendering it unavailable ()

(d) To gain unauthorized access to user accounts ()

3. What is a common use of a cryptographic hash function in computer security?

(a) Encrypting data so that it can be decrypted later ()

(b) Generating a fixed-size digital fingerprint to verify data integrity ()

(c) Compressing data to reduce storage requirements ()

(d) Randomly rearranging data to improve security ()

4. What is the main advantage of using a one-time pad for encryption?

(a) It relies on the computational difficulty of solving NP-hard problems to secure data ()

(b) It achieves unconditional (information-theoretic) security by using a truly random key that is as long as the message and used only once ()

(c) It minimizes key management challenges by allowing a short key to be securely reused for multiple messages ()

(d) It incorporates advanced data compression techniques to reduce ciphertext size and enhance security ()

5. Which of the following technologies is specifically designed to secure online credit card transactions by encrypting sensitive financial data?

(a) Secure Sockets Layer (SSL) ()

(b) Secure Electronic Transaction (SET) ()

(c) HTTP ()

(d) JavaScript ()

6. Which protocol is primarily used for sending e-mail messages from a client to a mail server?

- (a) Post Office Protocol (POP) ()
- (b) Simple Mail Transfer Protocol (SMTP) ()
- (c) Internet Control Message Protocol (ICMP) ()
- (d) Pretty Good Privacy (PGP) ()

7. Which type of Firewall operates at the network layer and filters traffic based on IP addresses, protocols and port numbers?

- (a) Packet Filtering Firewall ()
- (b) Stateful Inspection Firewall ()
- (c) Application-Level Gateway ()
- (d) Circuit-Level Gateway ()

8. In firewall design, which principle involves implementing multiple security measures to protect network resources, ensuring that if one layer fails, subsequent layers continue to provide protection?

- (a) Least privilege ()
- (b) Defense in depth ()
- (c) Default allow ()
- (d) Separation of duties ()

9. Which class does the IPv4 address 189.177.26.191 belong to?

- (a) Class A ()
- (b) Class B ()
- (c) Class C ()
- (d) Class D ()

10. In which layer of the TCP/IP model do the Internet Protocol (IP) and Internet Control Message Protocol (ICMP) operate?

- (a) Application layer ()
- (b) Transport layer ()
- (c) Internet layer ()
- (d) Network interface layer ()

II. Indicate whether the following statements are True (T) or False (F) by putting a Tick (✓) mark : $1 \times 5 = 5$

1. Non-repudiation ensures that once a transaction or communication has taken place, neither the sender nor the receiver can deny having participated in it.

(T / F)

2. Java and JavaScript are functionally equivalent programming languages that can be used interchangeably in web development.

(T / F)

3. In the RSA algorithm, if the public exponent (e) is chosen as 1, the encryption process will still be secured.

(T / F)

4. A screened subnet firewall configuration employs two packet-filtering routers and a bastion host to create an isolated subnetwork, enhancing security by adding multiple layers of defense.

(T / F)

5. Address Resolution Protocol (ARP) is a network protocol that maps a device's MAC address to its corresponding IP address.

(T / F)

III. Answer any five of the following : $2 \times 5 = 10$

1. Briefly explain the role of cookies in web browsers.

(8)

2. Explain the concept of a Demilitarized Zone (DMZ) in network security and discuss its significance in a screened subnet firewall configuration.

(9)

3. Compare and contrast Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models, highlighting their key differences and typical use cases.

(10)

4. Describe the concept of a substitution cipher and provide an example demonstrating its encryption process.

(11)

5. What is a Digital Signature and how does it ensure the authenticity and integrity of a message?

(12)

6. How does a TCP session hijacking attack compromise network security?

(13)

7. What is the primary function of Network Address Translation in networking?
