.

Printed Page:-4 **Subject Code:- BCSCY0502**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute Affiliated to AKTU, Lucknow)
B.Tech
SEM: V - THEORY EXAMINATION (2025 - 2026)
Subject: Network Security and Cryptography

Time: 3 Hours **Max. Marks: 100**

General Instructions:

IMP: *Verify that you have received the question paper with the correct course, code, branch etc.*

1. *This Question paper comprises of* ***three Sections -A, B, & C.*** *It consists of Multiple Choice Questions (MCQ's) & Subjective type questions.*

2. *Maximum marks for each question are indicated on right -hand side of each question.*

3. *Illustrate your answers with neat sketches wherever necessary.*

4. *Assume suitable data if necessary.*

5. *Preferably, write the answers in sequential order.*

6. *No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.*

SECTION-A 20

1. Attempt all parts:-

1-a. Identify the principle of the CIA triad that ensures data is accessible to authorized users when needed. (CO1,K1) 1

(a) Confidentiality
(b) Integrity
(c) Availability
(d) Authenticity

1-b. Classify a software flaw that is unknown to the vendor and has no available patch.(CO1,K2) 1

(a) Phishing
(b) Zero-day vulnerability
(c) SQL Injection
(d) Ransomware

1-c. Identify the branch of cryptology that focuses on the science of breaking cryptosystems.(CO2,K1) 1

(a) Cryptography
(b) Cryptanalysis
(c) Steganography
(d) Encryption

1-d. Classify the Caesar Cipher based on its primary operation.(CO2,K2) 1

(a) Transposition Cipher
(b) Asymmetric Cipher
(c) Substitution Cipher

(d) Stream Cipher

1-e. Identify the protocol that ensures secure communication at the transport layer of the OSI model.(CO3,K1) 1

(a) TLS
(b) FTP
(c) SMTP
(d) Telnet

1-f. Identify the IPsec protocol that provides encryption along with authentication.(CO3,K1) 1

(a) AH
(b) ESP
(c) ICMP
(d) ARP

1-g. Identify the attack technique that intercepts and potentially alters communications between two parties.(CO4,K1) 1

(a) Denial of Service
(b) Man-in-the-Middle (MitM)
(c) SQL Injection
(d) Port Scanning

1-h. Primary benefit of signature-based IDS systems.(CO4,K1) 1

(a) Detection of zero-day anomalies without prior data
(b) Low false positive rate for known threats
(c) Automatic behavior baselining
(d) Inherent encrypted traffic inspection

1-i. Major benefit of network segmentation:(CO5,K1) 1

(a) Faster download speeds
(b) Reducing power usage
(c) Limiting the spread of an attack
(d) Improving screen resolution

1-j. Primary goal of the Principle of Least Privilege:(CO5,K1) 1

(a) To make users happy
(b) To reduce network speed
(c) To limit access and reduce risk
(d) To save disk space

2. Attempt all parts:-

2.a. Differentiate between a virus and a worm.(CO1,K4) 2

2.b. Differentiate between a block cipher and a stream cipher.(CO2,K4) 2

2.c. Summarize the main purpose of TLS in securing network communication.(CO3,K2) 2

2.d. Define Denial of Service (DoS) in one sentence.(CO4,K1) 2

2.e. Explain with an example of a network segmentation technique (VLANs, subnets).(CO5,K2) 2

.

SECTION-B 30

3.a. Answer any one of the following:-

3.a.(i)	Explain the three core principles of the CIA triad with a suitable example for each.(CO1,K2)	6
3.a.(ii)	Compare and contrast the three main types of firewalls: Packet-filtering, Stateful, and Proxy.(CO1,K4)	6

3.b. Answer any one of the following:-

3.b.(i)	Compare and contrast symmetric and asymmetric cryptography based on key management, speed, and primary use cases.(CO2,K4)	6
3.b.(ii)	Describe the steps involved in the key generation phase of the RSA algorithm.(CO2,K2)	6

3.c. Answer any one of the following:-

3.c.(i)	Sketch and explain a sequence diagram showing the TLS handshake process.(CO3,K3)	6
3.c.(ii)	Analyze the differences between AH and ESP protocols in IPsec with examples.(CO3,K4)	6

3.d. Answer any one of the following:-

3.d.(i)	Contrast signature-based and anomaly-based IDS in terms of detection capability and maintenance.(CO4,K4)	6
3.d.(ii)	Discuss firewall policy design principles to minimize rule conflicts while enforcing segmentation.(CO4,K2)	6

3.e. Answer any one of the following:-

3.e.(i)	Explain demilitarized zone (DMZ) in networking.(CO5,K2)	6
3.e.(ii)	Analyze NAC in network security.(CO5,K4)	6

SECTION-C 50

4. Answer any one of the following:-

4-a.	Explain the core principles, goals, and objectives of network security. Discuss how security policies and mechanisms like firewalls and access control work together to achieve these goals.(CO1,K2)	10
4-b.	Classify and describe various categories of threats and attacks, including Malware, DoS/DDoS, and Insider Threats. For each category, suggest a relevant security mechanism for prevention and detection.(CO1,K2)	10

5. Answer any one of the following:-

5-a.	Describe the complete structure and operation of the DES algorithm, including its key schedule, Feistel function, and the role of S-boxes and P-boxes.(CO2,K2)	10
5-b.	Explain the AES encryption process in detail for a 128-bit key. Your answer should cover all layers (Byte Sub, ShiftRows, MixColumn, Key Addition) and the key expansion process.(CO2,K2)	10

6. Answer any one of the following:-

6-a.	Analyze IPsec architecture and explain AH and ESP with examples of use cases.(CO3,K4)	10
6-b.	Illustrate VPN setup for both site-to-site and remote access, highlighting security	10

protocols.(CO3,K3)

7. Answer any one of the following:-

7-a.	Explain the concept of defense-in-depth and list its main security layers in an enterprise network.(CO4,K2)	10
7-b.	Explain the difference between IDS and IPS and where each should be placed in a typical enterprise network.(CO4,K2)	10

8. Answer any one of the following:-

8-a.	Outline a network architecture design for an hospital with example of each steps.(CO5,K4)	10
8-b.	Analyze the network segmentation as a security control along with its practical implementation using VLANs.(CO5,K4)	10