Pimpri Chinchwad Education Trust's

Pimpri Chinchwad College of Engineering (PCCoE)

(An Autonomous Institute)
Affiliated to Savitribai Phule Pune University(SPPU)
ISO 21001:2018 Certified by TUV SUD

CNS: Question Bank

Class : Third Year (All Division) **Academic Year: 2025 - 2026** **Semester: I**
Course: Computer Networks and Security **Course code: BCE25PC03**
Module: Networks and Security

UNIT I: Basic of Networking

Sr. No	Questions	Difficulty Level	Blooms Level
1	Use a block diagram to show how a communication system transmits a signal.	Medium	Apply
2	List the seven layers of the OSI model from Layer 1 to Layer 7.	Basic	Remember
3	Classify a given network scenario as LAN, WAN, MAN, or PAN and justify your choice.	Medium	Apply
4	How would you identify the role of the Physical Layer when troubleshooting a network connectivity issue?	Medium	Apply
5	How would you decide which network architecture Client-Server or Peer-to-Peer is more suitable for a small office setup?	Medium	Apply
6	List and explain any three common physical network topologies.	Basic	Understand
7	Describe the working of Fiber Optic Cable.	Basic	Understand
8	What is the primary purpose of framing at the Data Link Layer?	Basic	Remember
9	How would you apply flow control and error control mechanisms to improve data transmission over a noisy network?	Medium	Apply
10	Given a data stream, how would you use a single parity bit to detect errors? What problems might you still encounter?	Medium	Apply

11	Can you identify a real-life situation where a Simplex protocol would be the best communication method? Explain why.	Medium	Apply
12	You are troubleshooting a network issue where devices are failing to access the transmission medium properly, and logical communication between devices is inconsistent. Based on the IEEE 802 standard, determine which sublayer(s) of the Data Link Layer are likely responsible for these issues and explain how each contributes to resolving them.	Medium	Apply
13	List types of framing. Describe variable size framing in detail.	Basic	Understand
14	Compare and contrast the primary advantages and disadvantages of a Star topology versus a Bus topology.	Medium	Analyze
15	Explain the key differences between a network switch and a router. Your answer should include the OSI layer at which each device operates and the type of address (MAC or IP) each uses to make forwarding decisions.	Medium	Analyze
16	Why Fiber Optic cable is generally preferred over Unshielded Twisted-Pair (UTP) cable for long-distance, high-bandwidth backbone connections between buildings?	Medium	Apply
17	Compare persistent and non-persistent HTTP connections in terms of efficiency and resource utilization.	Medium	Analyze
18	Draw TCP/IP model by explaining the primary function of each of its four layers.	Medium	Analyze
19	Explain the concept of network addressing by differentiating the purpose of a physical address (MAC address) from a logical address (IP address).	Medium	Analyze
20	List and explain various addresses supported by TCP/IP model	Medium	Analyze
21	In a situation where multiple network layer protocols need to share a single data link, explain how the LLC sublayer facilitates this and apply its functions to manage data flow between these protocols.	Medium	Apply
22	A network administrator needs to optimize data transmission over a high-latency link. Apply your understanding of Stop-and-Wait and Sliding Window protocols to recommend the more efficient method, supporting your decision with reasoning based on channel utilization and efficiency.	Medium	Apply

23	A protocol designer is implementing the Selective Repeat ARQ in a communication system. Apply the rule for determining the appropriate window size to calculate the maximum sender window, given a specific sequence number range.	Medium	Apply
24	In designing a Go-Back-N ARQ protocol, apply the window size formula to determine the maximum allowable sender window size if the sequence number field is 4 bits long.	Medium	Apply
25	A sender needs to transmit the data word 110101 using CRC. If the generator polynomial is (represented as 1001), calculate the CRC checksum and determine the final codeword to be transmitted.	Medium	Apply
26	A network technician is tasked with selecting an error detection method for a noisy communication channel that frequently experiences burst errors. Apply your knowledge of Cyclic Redundancy Check (CRC) to justify its suitability over parity checking in this scenario.	Medium	Apply
27	Consider a scenario where the sender wants to send the message 110110101 to the another side using CRC-3 code where the generator polynomial for division is X3+X+1. Show the error free transmission as well as error full transmission by considering error at the left most bit i.e a8 bit (110110101).	Medium	Apply
28	During data transmission using Stop-and-Wait ARQ, a lost acknowledgment results in repeated frame transmission. Apply the concepts of sequence numbers and timers to explain how the receiver and sender resolve this issue and ensure correct data delivery.	Medium	Apply
29	A system designer is configuring a reliable data transmission protocol using Sliding Window. Apply your understanding of sender and receiver window roles to determine how adjusting window sizes can optimize flow control and prevent buffer overflows.	Medium	Apply
30	A company plans to expand its network infrastructure. Given the need for both scalability and fault tolerance, apply your understanding of Mesh and Star topologies to recommend the most suitable design, justifying your decision with practical considerations.	Medium	Apply
31	If the unit exchanged at the data link layer level is called a frame and the unit exchanged at the network level is called a packet, do frames encapsulate packets or do packets encapsulate frames? Show how a piece of data is passed down from the Application Layer through to the Physical Layer of the OSI model.	Medium	Apply

32	Critically evaluate this statement: "Because modern networks are built using the TCP/IP protocol suite, the seven-layer OSI model is purely a theoretical concept with no practical value for network engineers."	High	Evaluate
33	Describe the theoretical process of how a packet is forwarded between two separate LANs. Your explanation must detail the distinct and unchanging roles of the source and destination IP addresses versus the dynamically changing roles of the source and destination MAC addresses at each hop.	High	Analyze
34	In the context of the client-server model, what is a "single point of failure"? Justify two distinct theoretical strategies that can be implemented in a network's design to mitigate this risk.	High	Evaluate
35	Critically evaluate the suitability of the Stop-and-Wait protocol for a network characterized by a long propagation delay and a high data rate (i.e., a high bandwidth-delay product), such as a satellite link. Justify your conclusion.	High	Evaluate
36	You need to set up a WIRED network comprising 30 systems for a small office environment. Each system will need to communicate with one another for file sharing, printer access, and internet connectivity. Provide the configuration details for this network. Additionally, explain which network topology would be most suitable to minimize traffic problems in this scenario.	Medium	Apply
37	A protocol designer is implementing a Sliding Window protocol using 3-bit sequence numbers. Apply your understanding of the relationship between sequence number bits and window size to determine the maximum safe window size. What issue might occur if the window size exceeds this limit during transmission?	High	Apply
38	Imagine you're tasked with improving the efficiency of a basic Stop-and-Wait protocol in a high-latency network environment. Without using the full complexity of the Sliding Window protocol, propose a conceptual modification that allows more than one frame to be "in-flight" at a time. Describe how your modified protocol would work, including how it manages acknowledgments and ensures reliable delivery.	High	Apply

UNIT II: TCP/IP Model			
Sr.No	**Questions**	**Difficulty Level**	**Blooms Level**
1	Demonstrate how the fields in an IPv4 header are used to deliver a packet from source to destination.	Basic	Analyze
2	Demonstrate how IPv4 and IPv6 headers are structured differently in practical network communication.	Medium	Analyze
3	Evaluate the responsibilities of the network layer in the OSI model with regard to data routing and addressing.	Medium	Evaluate
4	Examine the operational mechanism of the RIP protocol and its limitations in modern networks.	Medium	Analyze
5	Analyze the OSPF protocol's link-state operation and its approach to path selection.	Medium	Analysis
6	Explain BGP's operational principles and explain how path selection occurs between autonomous systems.	Basic	Understand
7	Discuss the concept of sockets in the transport layer and their role in establishing reliable communication.	High	Create
8	Differentiate TCP and UDP in terms of reliability, overhead, and suitability for different applications.	Basic	Understand
9	Examine the TCP header structure and interpret the function of each field in maintaining connection reliability.	Medium	Analyze
10	Analyze the UDP header and explain the role of its fields in connectionless communication.	Medium	Analyze
11	Assess how TCP flow control manages the rate of data transmission between sender and receiver.	Medium	Evaluate
12	Analyze TCP congestion control mechanisms and their effects on network traffic management.	Medium	Analyze
13	Outline HTTP's purpose in networking and its role in client-server interactions.	Basic	Understand

14	Compare persistent and non-persistent HTTP connections in terms of efficiency and resource utilization.	Basic	Understand
15	Discuss the structure of HTTP request and response messages and identify critical components.	Medium	Understand
16	Evaluate how cookies and caching mechanisms influence HTTP session management and web performance.	High	Evaluate
17	Summarize SMTP protocol operations and assess its role in reliable email transmission.	Medium	Understanding
18	Examine DNS operations and discuss how it resolves domain names to IP addresses.	Medium	Analyze
19	Analyze DHCP’s client-server operation and its role in dynamic IP allocation.	Medium	Analyze
20	Compare FTP and Telnet protocols, highlighting their purposes and operational differences.	Medium	Analyze
21	Discuss RIP, OSPF, and BGP regarding scalability, convergence speed, and network efficiency.	Medium	Evaluate
22	Differentiate connection-oriented and connectionless transport protocols in terms of reliability and overhead.	Basic	Understanding
23	Deconstruct the TCP three-way handshake and identify critical stages ensuring connection establishment.	Medium	Understanding
24	Classify sliding window protocol in TCP and analyze its impact on data flow control.	Medium	Analyze
25	Assess the effects of network congestion and critically evaluate techniques for its control.	Medium	Evaluate
26	Formulate a simple client-server socket communication setup and propose a measure to enhance reliability.	High	Create
27	Compare IPv4 and IPv6 headers and addressing methods in terms of efficiency and scalability.	Medium	Understanding
28	Analyze the impact of packet loss on TCP and UDP applications and identify which is more resilient.	Medium	Analyze
29	Examine HTTP caching mechanisms and their importance in improving web application performance.	Medium	Analyze

30	Evaluate DHCP message types (Discover, Offer, Request, Ack) and their sequence during IP assignment.	Medium	Evaluate
31	Analyze the differences between RIP, OSPF, and BGP in terms of scalability, convergence, and efficiency.	Medium	Analyze
32	Analyze a TCP connection to identify scenarios leading to congestion collapse and performance degradation.	Medium	Analyze
33	Analyze the routing challenges in a dual-stack (IPv4/IPv6) environment and propose suitable solutions for interoperability.	Medium	Analyze
34	Analyze the performance of TCP and UDP for video streaming, highlighting strengths and weaknesses in real-time data delivery.	Medium	Analyze
35	Design a socket-based chat application and justify the choice of transport protocol for reliable communication.	High	Create
36	Analyze the effect of persistent vs non-persistent HTTP on page load times for high-traffic websites.	High	Analyze
37	Analyze different DHCP deployment approaches and their impact on network scalability and IP address management.	Medium	Analyze
38	Analyze the differences between DNS caching and resolution strategies and their impact on system performance under load.	Medium	Analyze
39	Analyze how FTP and HTTP differ in reliability and performance for file transfer over WANs.	High	Analyze
40	Examine a small network and determine routing tables using RIP given the network topology.	High	Analyze

<table>
<tr><th colspan="4">UNIT III: Basics of Security</th></tr>
<tr><th>Sr.No</th><th>Questions</th><th>Difficulty Level</th><th>Blooms Level</th></tr>
<tr><td>1.</td><td>State two major challenges in designing a secure system.</td><td>Basic</td><td>Remember</td></tr>
<tr><td>2.</td><td>Differentiate between a threat and a vulnerability with an example.</td><td>Basic</td><td>Understand</td></tr>
<tr><td>3</td><td>Given a scenario of network communication, identify whether each attack is passive or active, and justify your reasoning.</td><td>Basic</td><td>Apply</td></tr>
</table>

4	For the given a set of security incidents, classify each as an insider or outsider threat. Justify your classification based on access, intent, and potential damage. Incidents: An employee copies confidential files to a USB drive. A hacker gains access to the company server via phishing.	Basic	Apply
5	Given a simple encryption using a 16-bit key, outline how you would perform a brute-force attack to recover the key. Estimate how many attempts are required and discuss why this approach fails for 128-bit keys.?	Basic	Apply
6	Encrypt the word HELLO using a Caesar cipher with a shift of 2.	Basic	Apply
7	Illustrate data integrity with a simple example of file transfer between two computers	Basic	Understand
8	In a Caesar cipher with a shift of 4, what is the ciphertext for DATA?	Basic	Apply
9	Describe passive attacks in detail? Categorize each attack and explain with one example each.	Medium	Apply
10	Apply the CIA Triad principles to a real-world example, such as online banking or hospital record management. How would each element ensure system security?	Medium	Apply
11	Given a scenario where a company’s web server is flooded with traffic, apply your understanding of the CIA triad to determine which property is affected and how.	Medium	Apply
12	Given a scenario of a web application with outdated software, apply your understanding of vulnerabilities to identify possible security breaches. Explain how an attacker might exploit them.	Medium	Apply
13	Encrypt a short message ("SECURITY") using a given Playfair key table. Show each step and explain how the digraph substitution is applied.	Medium	Apply
14	Explain why availability can sometimes conflict with confidentiality in system design.	Medium	Analyze
15	Give an example where all three CIA properties are compromised simultaneously.	Medium	Analyze
16	Given a scenario where a company stores customer data online, identify a potential threat, describe a possible attack, and estimate the associated risk..	Medium	Apply
17	Explain the operational model of security using a simple diagram.	Medium	Understand
18	Analyze how Denial of Service (DoS) attacks affect the CIA triad.	Medium	Analyze
19	Given a network scenario where encrypted traffic passes through an unsecured Wi-Fi hotspot, apply your knowledge to identify how a Man In The Middle attack could occur and what information could be compromised.	Medium	Apply
20	Discuss limitations of traditional security approaches in modern networked systems.	Medium	Evaluate

21	Compare symmetric and asymmetric cryptography in terms of speed and security.	Medium	Analyze
22	The following ciphertext has been encrypted using a Caesar cipher: Ciphertext: KHOOR ZRUOG Apply cryptanalysis to recover the plaintext. Show your steps and explain how you determined the correct key.	Medium	Apply
23	Encrypt the message MEET AT NOON using a Caesar cipher with a shift of 3 and show the steps.	Medium	Apply
24	Decrypt the ciphertext KHOOR using a Caesar cipher with a shift of 3.	Medium	Apply
25	Encrypt the digraph HI using a Playfair cipher key table you create.	Medium	Apply
26	Demonstrate why frequency analysis can break substitution ciphers. Give a simple example using English letter frequencies.	Medium	Apply
27	Compare the Caesar cipher and Playfair cipher in terms of security and complexity.	Medium	Analyze
28	Explain how a security breach can impact business operations beyond just data loss.	Medium	Analyze
29	How does phishing exploit human behavior rather than technical vulnerabilities?	Medium	Analyze
30	Given a 5x5 Playfair key table, encrypt the digraphs “ME” and “ET”, showing all intermediate steps.	Medium	Apply
31	Given a scenario where two users need to communicate securely, apply symmetric and asymmetric cryptography. Show how keys are distributed in each case and explain the practical challenges for asymmetric key distribution.	Medium	Apply
32	Decrypt the ciphertext “RIJVS UYVJN” using a Caesar cipher with a shift of 4 and explain each step.	Medium	Apply
33	Analyze the strength of a 56-bit key in DES against modern brute-force attacks. How long would it take to break it, assuming 1 billion keys per second?	High	Analyze
34	A network is using RSA encryption. Discuss how choosing small primes for key generation can compromise security.	High	Analyze
35	Compare classical ciphers (Caesar, Playfair) and modern block ciphers (AES) in terms of computational complexity, key space, and resistance to attacks, giving examples.	High	Analyze
36	Explain a scenario where maintaining high availability could compromise confidentiality. How would you mitigate this conflict?	High	Evaluate
37	Explain how a multi-layered security approach enhances CIA in an enterprise network.	High	Evaluate
38	Discuss the consequences of ignoring integrity checks in a cloud storage system. Give suitable example.	High	Evaluate
39	Discuss why using small primes in RSA is insecure, including calculations showing potential vulnerabilities.	High	Analyze
40	Encrypt the message “SECURE DATA” using a Playfair cipher with a key of your choice and show all intermediate steps.	High	Apply

	A hospital stores sensitive patient data digitally. Propose a security strategy to protect confidentiality, integrity, and availability, considering both internal and external threats.	High	Create

UNIT IV: Symmetric and Asymmetric Cipher

Sr.No	Questions	Difficulty Level	Blooms Level
1	With a suitable diagram, describe stream ciphering in detail?	Basic	Understand
2	How a stream cipher encrypts data differently than a block cipher.	Basic	Understand
3	Encrypt the binary string "11010010" using a stream cipher where the key stream is "01101100". Show the step-by-step process.	Medium	Apply
4	Differentiate between block cipher and stream cipher.	Basic	Understand
5	Encrypt the plaintext "HELLO" using a block cipher with a block size of 5. Assume a basic substitution scheme and show the encryption process.	Medium	Apply
6	Explain the general structure of DES. How many rounds does the encryption process involve?	Medium	Analyze
7	Perform the first round of DES encryption on a given 64-bit plaintext using a DES structure and a 56-bit key. Show the initial permutation and first round's function (F-function).	Medium	Apply
8	Draw and explain the internal structure of single round of DES algorithm	Medium	Analyze
9	List the steps involved in DES key generation, including PC-1, shifts, and PC-2.	Basic	Understand
10	How permutation and substitution steps occur in DES algorithm	Basic	Understand
11	Compare and evaluate the security of stream ciphers vs. block ciphers in real-time data encryption. Which one would you recommend for a low-latency application and why?	Medium	Analyze
12	Discuss Feistel cipher structure in detail? Identify one example of a Feistel cipher.	Basic	Understand
13	Explain the key components of the Feistel cipher structure. How does the structure ensure decryption is the reverse of encryption?	Medium	Analyze
14	Demonstrate the encryption of a 4-bit message using a simple Feistel cipher with two rounds and a given key. Walk through each step.	High	Apply
15	Illustrate man in middle attack in DES. Explain in detail.	Basic	Understand
16	What is Double DES, and how does it differ from the standard DES?	Medium	Understand
17	Analyze the strengths and weaknesses of DES. Why DES considered secure in the 1970s, and what led to its vulnerabilities in modern times?	High	Analysis
18	Evaluate the effectiveness of triple DES (3DES) in addressing the vulnerabilities of DES. Does it fully mitigate the problems of DES, or does it have its own weaknesses?	High	Evaluation
19	Explain the concept of Triple DES (3DES). How does it improve upon the security of DES?	Basic	Understand

20	Generate cipher text for given plain text using DES algorithm. it is decided to use DES algorithm to provide confidentiality to the massage in transit. Generate total 16 sub keys of 48 bits each using DES algorithm. (supporting data will be provided)
	M = 0123456789ABCDEF
	K= 133457799BBCDFF1
		High	Apply

21	Compare symmetric and asymmetric cryptosystems in terms of security and efficiency.	Medium	Analyze
22	Analyze the vulnerability of Double DES to the Meet-in-the-Middle attack. Why is Double DES not as secure as originally thought?	Medium	Analyze
23	Compute the ciphertext using RSA for plaintext $P = 9$, given $p = 3$, $q = 11$, $e = 3$.	Medium	Apply
24	Derive the public and private keys in RSA with $p = 7$, $q = 13$, $e = 5$.	Medium	Apply
25	Analyze the role of the round function in the Feistel cipher. Why is it important that the round function is non-linear?	Medium	Analysis
26	Compute the shared secret key in the Diffie-Hellman protocol given $p = 23$, $g = 5$, $a = 6$, $b = 15$.	Medium	Apply
27	How a Man-in-the-Middle attack disrupts the Diffie-Hellman exchange.	Medium	Apply
28	Design a Feistel-based encryption system with 3 rounds. Explain how you would generate the subkeys and describe the encryption and decryption process.	High	Evaluation
29	Derive the public key and private key pair using RSA algorithm. Consider $p=17$, $q=23$, and $e = 5$. Also encrypt the message $M=2$ using the generated key.	Medium	Apply
30	Evaluate the effectiveness of public key cryptosystems in secure communication.	Medium	Analyze
31	Explain design principles of block cipher with suitable diagram.	Basic	Understand
32	Describe the purpose of S boxes in DES. Explain the Avalanche effect.	Basic	Understand
33	Apply sub key generation process in simplified DES algorithm with example.	Medium	Apply

Dr. G. B. Sambare

Course Owner and Course Coordinator **Module Coordinator**