Indian Institute of Technology, Kanpur
Computer Science and Engineering

End Semester Exam
CS425: Computer Networks

Instructor: Adithya Vadapalli

04/05/2025

Name: _____

Roll Number: _____

---

1. This exam contains 19 pages (including this cover page) and 8 questions.
2. Total of marks is 100.
3. You are allowed to bring one A4-sized cheat sheet, which is handwritten (by you!!) notes to the exam.
4. Please write your name in **ALL CAPS**. You have **120 minutes** to solve the exam.
5. Good luck!

Distribution of Marks

Question	Points	Score
1	10	
2	20	
3	9	
4	17	
5	10	
6	10	
7	12	
8	12	
Total:	100	

1. This question has 10 parts. Each of them is a true or false question. No need to give an explanation. There are no negative marks for wrong answers.

   (a) (1 point) NAT allows multiple devices in a private network to share a single public IP address when accessing the Internet.

   Solution: True. NAT (Network Address Translation) maps multiple private IP addresses to a single public IP address, allowing multiple internal hosts to share one IP when communicating with the internet.

   (b) (1 point) NAT devices change both source and destination IP addresses in a packet.

   Solution: False. NAT typically modifies only the *source IP address and port* when a packet leaves the private network. It does not change the destination IP unless performing destination NAT (DNAT), which is a different configuration.

   (c) (1 point) The Cyclic Redundancy Check (CRC) can detect all single-bit errors.

   Solution: True. CRC is designed to detect common types of errors, including *all single-bit errors*, assuming an appropriate generator polynomial is used.

   (d) (1 point) ALOHA protocol has a higher maximum efficiency than Slotted ALOHA.

   Solution: False. Slotted ALOHA is more efficient due to reduced collisions. Max efficiency: Pure ALOHA is 18.4 percent, Slotted ALOHA is 36.8 percent.

   (e) (1 point) TLS operates between the transport and application layers and provides end-to-end encryption.

   Solution: True. TLS resides between the transport and application layers and provides end-to-end encryption between client and server applications.

(f) (1 point) WEP provides strong authentication for Wi-Fi networks.

Solution: False. WEP is outdated and insecure. It uses weak encryption and key management, and does not provide strong authentication.

(g) (1 point) Diffie-Hellman is vulnerable to man-in-the-middle attacks if not authenticated.

Solution: True. Diffie-Hellman on its own lacks authentication, making it vulnerable to man-in-the-middle attacks unless combined with authentication mechanisms.

(h) (1 point) In TLS, the client authenticates the server using a digital certificate.

Solution: True. The server presents a digital certificate during the TLS handshake, and the client authenticates it using a trusted certificate authority.

(i) (1 point) Network Layer ensures that packets are transported reliably over an unreliable channel.

Solution: False. The Network Layer (e.g., IP) provides best-effort delivery. Reliable transport is handled by protocols at the Transport Layer (e.g., TCP).

(j) (1 point) Link State routing protocols use the Bellman-Ford algorithm to compute shortest paths.

Solution: False. Link State routing protocols (e.g., OSPF) use *Dijkstra's algorithm*, whereas *Bellman-Ford* is used in Distance Vector protocols (e.g., RIP).

2. Transport Layer Security (TLS), Tor, PGP, and SSH are widely used tools and protocols for securing communication. Answer the following questions. Color the box adjacent to the correct answer(s). For some questions, more than one answer could be correct. You have to mark all the correct answers to get credit.

(a) (2 points) What are the primary security goals of TLS? (Choose all that apply)

- [ ] Authentication
- [ ] Non-repudiation
- [ ] Confidentiality
- [ ] Integrity
- [ ] Availability

Solution:

- [x] Authentication
- [ ] Non-repudiation
- [x] Confidentiality
- [x] Integrity
- [ ] Availability

TLS provides authentication (typically of the server), confidentiality via encryption, and integrity via MACs or AEAD. It does not offer non-repudiation or guarantee availability.

(b) (2 points) In the TLS handshake, what type of key is typically used to encrypt the communication **after the handshake is complete**?

- [ ] Public key
- [ ] Private key
- [ ] Symmetric key
- [ ] None of the above

Solution:

- [ ] Public key
- [ ] Private key
- [x] Symmetric key
- [ ] Asymmetric key

TLS uses asymmetric cryptography to establish a shared symmetric key, which is then used for efficient data encryption.

(c) (2 points) How does TLS ensure the **integrity** of messages during communication?

- ☐ By using hashing algorithms and message authentication codes (MACs)
- ☐ By using public key encryption
- ☐ By using digital certificates
- ☐ By performing the handshake

Solution:

- ☑ By using hashing algorithms and message authentication codes (MACs)
- ☐ By using public key encryption
- ☐ By using digital certificates
- ☐ By performing the handshake

TLS uses MACs or AEAD (Authenticated Encryption with Associated Data) to ensure data integrity during transmission.

(d) (2 points) What role do **digital certificates** play in the TLS handshake?

- ☐ They encrypt the data
- ☐ They verify the server's identity
- ☐ They provide a shared secret key
- ☐ They prevent the use of weak encryption algorithms

Solution:

- ☐ They encrypt the data
- ☑ They verify the server's identity
- ☐ They provide a shared secret key
- ☐ They prevent the use of weak encryption algorithms

Digital certificates allow the client to verify that the server is the legitimate owner of the public key it presents.

(e) (2 points) What is the primary purpose of the **Tor** network?

- ☐ To accelerate internet speed using multiple paths
- ☐ To block malware and phishing attacks

☐ To perform encrypted email communication
☐ To enable anonymous communication over the internet

Solution:

☐ To accelerate internet speed using multiple paths
☐ To block malware and phishing attacks
☐ To perform encrypted email communication
☑ To enable anonymous communication over the internet

Tor provides anonymity by routing traffic through multiple relays and using layered encryption.

(f) (2 points) In the **Tor** network, what is the correct sequence of nodes that traffic passes through?

☐ Middle relay → Entry node → Exit node
☐ Exit node → Entry node → Middle relay
☐ Entry node → Middle relay → Exit node
☐ Middle relay → Exit node → Entry node

Solution:

☐ Middle relay → Entry node → Exit node
☐ Exit node → Entry node → Middle relay
☑ Entry node → Middle relay → Exit node
☐ Middle relay → Exit node → Entry node

Tor uses a three-hop circuit: Entry node → Middle relay → Exit node.

(g) (2 points) What is the main function of **PGP** in secure communications?

☐ Preventing denial-of-service attacks
☐ Encrypting and signing email messages
☐ Establishing a VPN connection
☐ Preventing data exfiltration

Solution:

- ☐ Preventing denial-of-service attacks
- ☑ Encrypting and signing email messages
- ☐ Establishing a VPN connection
- ☐ Preventing data exfiltration

PGP is primarily used to ensure confidentiality and authenticity of email via encryption and digital signatures.

(h) (2 points) Which of the following is a core security property provided by **Off-the-Record (OTR) Messaging**?

- ☐ Message authenticity using digital signatures that can be verified later
- ☐ Perfect forward secrecy and deniable authentication
- ☐ Centralized key management for user identities
- ☐ Long-term non-repudiation for audit purposes

Solution:

- ☐ Message authenticity using digital signatures that can be verified later
- ☑ Perfect forward secrecy and deniable authentication
- ☐ Centralized key management for user identities
- ☐ Long-term non-repudiation for audit purposes

OTR Messaging ensures that each session has its own ephemeral keys (perfect forward secrecy) and provides authentication without verifiable signatures, enabling deniability.

(i) (2 points) Which of the following best describes the primary use of **SSH**?

- ☐ Accessing web pages securely
- ☐ Secure remote login to a server
- ☐ Encrypting file systems
- ☐ Creating anonymous communication tunnels

Solution:

- [ ] Accessing web pages securely
- [x] Secure remote login to a server
- [ ] Encrypting file systems
- [ ] Creating anonymous communication tunnels

SSH is used to securely access and manage remote machines, typically through command-line access.

(j) (2 points) During the initial **SSH** handshake, how is the server's identity typically established?

- [ ] Symmetric key exchange
- [ ] Challenge-response over plaintext
- [ ] Server's public key authentication
- [ ] DNS over HTTPS

Solution:

- [ ] Symmetric key exchange
- [ ] Challenge-response over plaintext
- [x] Server's public key authentication
- [ ] DNS over HTTPS

The SSH client verifies the server's identity by checking its public key against a known host file or asking the user to confirm it.

3. A 4×4 block of data was transmitted using even parity in both row and column directions. The original data and its corresponding parity bits were arranged in the following 5×5 matrix. The last row and column contain the parity bits for the columns and rows, respectively; the bottom-right cell is the overall parity bit:

   (Note: The vertical bar separates the row data from the row parity bit. The last row contains column parity bits and the overall parity bit. The horizontal bar separates the column data from the column parity bit.)

   Upon reception, the following matrix was observed:

	Column 1	**Column 2**	**Column 3**	**Column 4**	**Row Parity**
Row 1	1	0	1	1	1
Row 2	0	1	1	0	1
Row 3	1	1	1	0	1
Row 4	0	0	1	1	0
Column Parity	0	1	0	0	0

   (a) (5 points) Identify the position (which row and column) of the error using 2-D parity analysis. Correct the error and write the corrected 4×4 data block.

   Solution: We check each row and column for parity mismatches:
   Compare original and received: - Row 2: original parity = 1, received parity = 0 $\rightarrow$ mismatch - Column 2: original parity = 1, received parity = 0 $\rightarrow$ mismatch
   So, the error is at intersection of Row 2 and Column 2, i.e., position (2,2) (0-based indexing). **Answer: Error is at position (2,2)**. Corrected matrix:

$$\begin{matrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{matrix}$$

(b) (2 points) Can single-bit errors be corrected using single-dimensional parities?

Solution: No

(c) (2 points) Can two-bit errors be corrected using two-dimensional parities?

Solution: No

4. Consider a datagram network using **12-bit host addresses**. A router uses **longest-prefix matching** to determine the appropriate interface for forwarding. The router has the following forwarding table:

Prefix Match (binary)	Interface
1	1
110	2
1101	3
11011	4
010	5
0100	6
0001	7
`otherwise`	8

Answer the following questions based on this table:

(a) (3 points) A datagram arrives at the router with destination address `110110101011`. To which interface will this datagram be forwarded?

Solution: The address starts with `11011`, which matches the longest prefix `11011` in the table. So, it will go to interface 4.

(b) (3 points) A datagram arrives at the router with destination address `010011001100`. To which interface will this datagram be forwarded?

Solution: The address starts with `0100`, which matches the prefix `0100` (longer than `010`). So, it will go to interface 6.

(c) (3 points) A datagram arrives at the router with destination address `111000110101`. To which interface will this datagram be forwarded?

Solution: The address starts with `1`, but does not match any longer prefix like `110`, `1101`, or `11011`. So, it matches `1` and goes to interface 1.

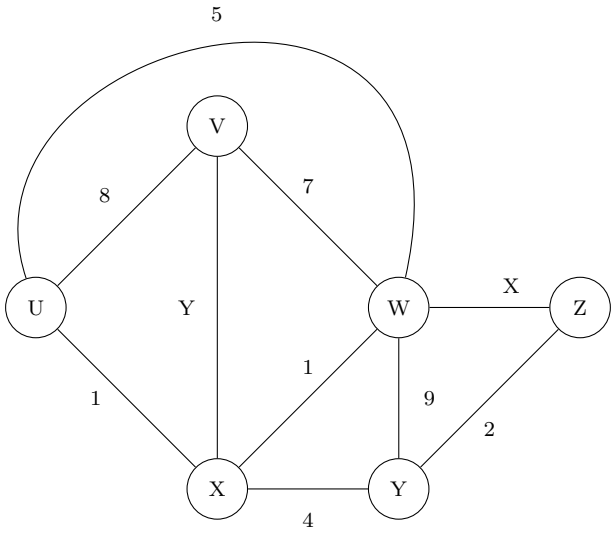
(d) (4 points) Provide an example of a 12-bit destination address that would match **both** the prefix `1101` and `110`, and explain (in one short sentence) why the router chooses the interface it does.

Solution: Example: `110100110011` matches both `110` and `1101`. Since `1101` is longer than `110`, the router uses the longest-prefix match and forwards the datagram to interface 3.

(e) (4 points) Suppose the prefix `0100` is removed from the table. How would that affect the forwarding decision for a datagram with destination address `010011111000`?

Solution: Without the `0100` prefix, the longest match is now `010`, which maps to interface 5. Previously, it would have matched `0100` and gone to interface 6. So now, it goes to interface 5.

5. Consider the incomplete 6-node network shown below, with the given link costs.



Completed table for shortest distance to all nodes **from X using Dijkstra's algorithm:**

Node	**Shortest distance from X**	**Previous Node**
X	0	n/a
U	1	X
W	1	X
V	3	X
Y	4	X
Z	6	Y

(a) (5 points) For link X, what is the cost associated with this link? If the answer can't be determined given the information, respond with `n/a`.

Solution: Because the link is never used, we cannot determine the value of X, so the answer is n/a.

(b) (5 points) For link Y, what is the cost associated with this link? If the answer can't be determined given the information, respond with `n/a`.

Solution: The prior node in the path to V is X, and we know the shortest distance of both V (3) and X (0), so 3 - 0 = 3, which is Y.

6. For this question, look at Figure 1. The IP and MAC addresses are shown for nodes A, B, C, and D, as well as for the router's interfaces. Consider an IP datagram being sent from node D to node C.

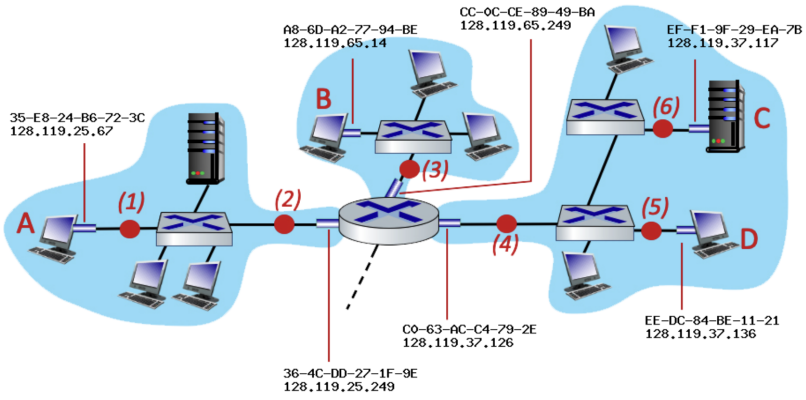


Figure 1: The Network Setup

(a) (2 points) What is the source MAC address at point 5?

Solution: The source MAC address at point 5 is EE-DC-84-BE-11-21

(b) (2 points) What is the destination MAC address at point 5?

Solution: The destination MAC address at point 5 is EF-F1-9F-29-EA-7B

(c) (2 points) What is the source IP address at point 5?

Solution: The source IP address at point 5 is 128.119.37.136

(d) (2 points) What is the destination IP address at point 5?

Solution: The destination IP address at point 5 is 128.119.37.117

(e) (2 points) Do the source and destination MAC addresses change at point 6? Answer with yes or no.

Solution: No, datagrams can be sent across the subnet via the link layer in one go.

7. A learning switch has four ports and starts with an empty forwarding table. It receives the following sequence of Ethernet frames:

Frame #	**Source MAC**	**Destination MAC**	**Port Received On**
1	A1	B1	1
2	B1	A1	2
3	C1	B1	3
4	D1	E1	4

(a) (4 points) After processing all four frames, what is the final state of the switch's forwarding table? Fill in the table below: *(1 mark for each row).*

MAC Address	Port
_____	_____
_____	_____
_____	_____
_____	_____

(b) (8 points) For each frame, state whether it will be **flooded** or **forwarded**, and if forwarded, to which port. *(2 marks for each row. A row must be completely correct to receive credit. For example, if the action "Forwarded" is correct but the port to which it is forwarded is incorrect, you will receive 0 out of 2 marks for that row.)*

Frame #	Action (Flooded / Forwarded to Port X)
_____	_____
_____	_____
_____	_____
_____	_____

Solution:

(a) **Final state of the switch's forwarding table:**

MAC Address	Port
A1	1
B1	2
C1	3
D1	4

Explanation: The switch learns the source MAC address and the incoming port for each frame. Since all sources are unique, each new frame adds a new entry.

(b) **Action for each frame:**

Frame #	Action (Flooded / Forwarded to Port X)
1	Flooded
2	Forwarded to Port 1
3	Forwarded to Port 2
4	Flooded

Explanation:

- **Frame 1:** Destination `B1` unknown ⇒ Flooded. Learns `A1` on port 1.
- **Frame 2:** Destination `A1` known ⇒ Forwarded to port 1. Learns `B1` on port 2.
- **Frame 3:** Destination `B1` known ⇒ Forwarded to port 2. Learns `C1` on port 3.
- **Frame 4:** Destination `E1` unknown ⇒ Flooded. Learns `D1` on port 4.

8. Alice wants to send a secure message M to Bob over an insecure channel. She wants to ensure the following:

   - Only Bob can read the message (**Confidentiality**)
   - Bob can verify that Alice sent the message (**Authentication**)
   - Bob can detect if the message was tampered with (**Integrity**)

   Assume:

   - Alice has Bob's public key: K_B^{pub}
   - Bob has Alice's public key: K_A^{pub}

   (a) (8 points) Match each of Alice's steps with its correct description.

Step	Description	Purpose (Match)
A	Compute $h = \text{Hash}(M)$	(i) Provide confidentiality
B	Compute $\sigma = \text{Sign}_{K_A^{\text{priv}}}(h)$	(ii) Provide authentication
C	Compute $C = \text{Enc}_{K_B^{\text{pub}}}(M, \sigma)$	(iii) Send the encrypted message over network
D	Send ciphertext C to Bob	(iv) Check integrity

   Answer: A–_____, B–_____, C–_____, D–_____

   Solution: Answer: A– iv), B– ii) , C– i), D– iii)

   (b) (4 points) Bob receives a ciphertext C that contains a message M and a digital signature σ. The table below lists four steps Bob may perform to process the ciphertext.

Step	Description
A	Compute $h' = \text{Hash}(M)$
B	Extract M and σ
C	Verify $\text{Verify}_{K_A^{\text{pub}}}(\sigma, h')$
D	Decrypt C using K_B^{priv}

What is the correct order in which Bob should perform the above steps to verify the authenticity and integrity of the message? Write the correct sequence of step labels (e.g., A $\rightarrow$ B $\rightarrow$ ...). *You will not receive any partial credit in this question. It is all or nothing.*

Solution: Answer: D $\rightarrow$ B $\rightarrow$ A $\rightarrow$ C