	Q. No. 2 (CLO 2)	25 Marks
	A software company is migrating its infrastructure to the cloud to improve scalability and cost-efficiency. However, a risk assessment reveals concerns about data breaches, insider threats, and compliance with international security standards. **Questions:** 1. Identify the key risks associated with cloud migration in this scenario. 2. Use a risk management framework to outline steps for identifying, assessing, and mitigating these risks. 3. Recommend specific cloud security controls (e.g., encryption, access control, monitoring) to address the identified risks.	10+10+5

	Q. No. 3 (CLO 2)	25 Marks
	A financial institution uses asymmetric encryption to secure online banking transactions. During an internal audit, it is discovered that private keys are stored on an unsecured server accessible to multiple employees, creating a significant security risk. **Questions:** 1. Analyze the risks associated with improper storage of private keys in this scenario. 2. Propose a secure key management strategy to mitigate these risks. 3. Explain how certificate authorities and digital certificates can enhance trust and security in this system	10+10+5

	Q. No. 4 (CLO 3)	25 Marks
	A company suspects an employee of leaking sensitive financial data to external parties. The IT department has been asked to conduct a digital forensic investigation to gather evidence and identify the source of the breach. **Questions:** 1. Explain the need for digital forensics in this scenario and the importance of preserving evidence integrity. 2. Describe the key phases of the digital forensics process that would be followed to investigate this incident. 3. Discuss the challenges that investigators may face during the investigation and recommend best practices to overcome these challenges.	10+5+5+5

********** End of Question Paper **********

Air University

Final Examination: Fall 2024
(To be solved on Answer Books only)

Student ID : [redacted]

Subject: Introduction to Cyber Security
Class: BS-CYS
Section(s): A [redacted]
Course Code: CY-104

Time Allowed: 2 ½ Hrs
Max Marks: 100
FM's Name: Muhammad Jalal Shah
FM's Signature:

INSTRUCTIONS

- Attempt responses on the answer book only.
- Nothing is to be written on the question paper.
- Rough work or writing on question paper will be considered as use of unfair means.

	Q. No. 1 (CLO 1)	25 Marks
	The diagram below represents the network infrastructure of a small organization, where employees communicate with a Central Server for data processing. The organization is facing two key challenges: 1. End systems are vulnerable to malware attacks. 2. Secure end-to-end communication between the clients and the Central Server must be ensured while restricting external traffic so that it only reaches the Central Server through a secure and monitored pathway.	
	Questions:	10+5+5+5
	Select and deploy the specific security technologies to: • Protect the end systems against malware attacks. • Enable secure end-to-end communication between clients and the Central Server. • Restrict and monitor external traffic that is directed towards central server • Draw a diagram to explain the deployment of security technologies.	

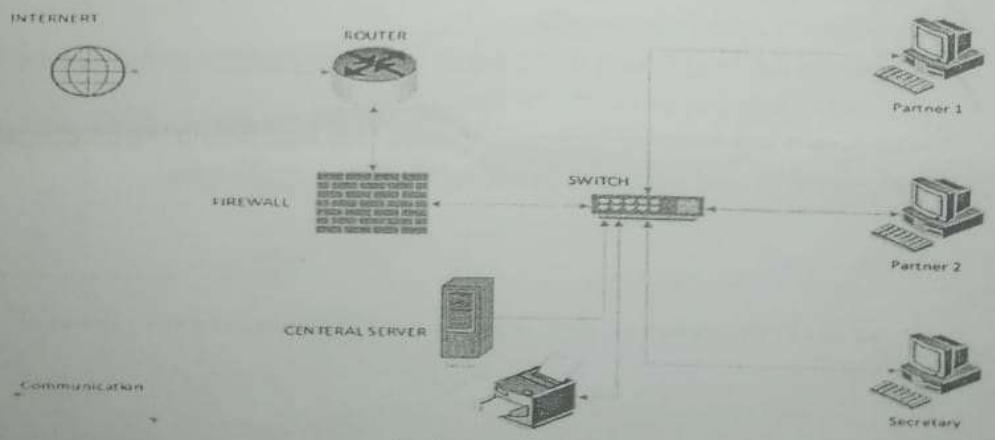

Fig. Network Diagram