Reg. No. : | | | | | | | | | | | | |

Question Paper Code:U2304

M.E. DEGREE EXAMINATION, APRIL / MAY 2025

Second Semester

Computer Science and Engineering

21PCS204- NETWORK SECURITY

(Regulations 2021)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART – A (5 x 20 = 100 Marks)

1.	(a)	Explain the concepts of "block size" and "padding." Why is it important to ensure that data is appropriately padded before encryption and what are the potential issues if padding is not handled correctly?	CO2- App	(20)
		Or		
	(b)	Discuss the trade-offs between the Advanced Encryption Standard (AES) and RSA encryption in terms of performance, security, and use cases. Under what circumstances would you choose AES over RSA and vice versa?	CO2- App	(20)
2.	(a)	How does the discrete logarithm problem serve as the foundation for the security of cryptosystems like the Diffie-Hellman key exchange? Explain the difficulty of solving this problem and how it impacts the choice of cryptographic parameters.	CO2- App	(20)
		Or		
	(b)	Explain the advantages of using Elliptic Curve Cryptography (ECC) over traditional public key algorithms like RSA, particularly in terms of key size and computational efficiency. How does this impact its adoption in resource-constrained environments like mobile devices?	CO2- App	(20)
3.	(a)	What are the primary goals of IPsec, and how does it differ from other security protocols such as SSL/TLS or SSH in terms of scope and implementation? Provide an example of where IPsec would be preferred over other protocols.	CO2- App	(20)
		Or		

	(b)	If a network administrator is configuring IPsec with AH in a secure communication setup, what additional security measures should they consider, given that AH does not provide encryption? How would you secure sensitive data in transit while still ensuring integrity and authentication using AH?	CO2- App	(20)
4.	(a)	Suppose you are designing a web application for an online banking system. How would you ensure that the system meets security requirements such as data integrity, confidentiality, and user authentication? What tools and techniques would you use to protect against man-in-the-middle (MITM) attacks and unauthorized data access?	CO2- App	(20)
		Or		
	(b)	An online store uses SSL to secure transactions between customers and the web server. How does SSL ensure the confidentiality and integrity of data during transmission, and what are the potential security risks if SSL is not properly configured (e.g., weak ciphers, expired certificates)?	CO2- App	(20)
5.	(a)	Consider a scenario where you need to protect a web application running on a public-facing server. How would you configure your firewall to allow legitimate web traffic while blocking common attack vectors like SQL injection and cross-site scripting (XSS)?	CO2- App	(20)
		Or		
	(b)	An employee in your organization has reported a virus infection. How would you conduct an incident response to remove the virus, and what steps would you take to ensure that similar infections do not occur in the future?	CO2- App	(20)