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

Question Paper Code: U5205

M.E. DEGREE EXAMINATION, APRIL / MAY 2025

Second Semester

Communication Systems

21PCM505- COMMUNICATION NETWORK SECURITY

(Regulations 2021)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART - A (5 x 20 = 100 Marks)

1.	(a)	Convert "MEET ME" using Hill cipher with the key matrix $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ Convert the cipher text back to plaintext	CO3- App	(20)
		Or		
	(b)	Encrypt the following using play fair cipher using the keyword MONARCHY " SWARAJ IS MY BIRTH RIGHT". Use X as blank space.	CO3- App	(20)
2.	(a)	For each of the following elements of DES, indicate the comparable element in AES if available. i) XOR of subkey material with the input to the function. ii) f function. iii) Permutation p. iv) Swapping of halves of the block.	CO4-App	(20)
		Or		
	(b)	How can the DES algorithm be applied in practice? Can you illustrate the process with an example that shows how data is encrypted and decrypted using DES?	CO4-App	(20)

3.	(a)	Describe about Hash Function. How its algorithm is designed? Explain its features & Properties?	CO1-U	(20)
		Or		
	(b)	In what order should the signature function and the confidentiality function be applied to a message, and why? Explain it with an appropriate example.	CO1-U	(20)
4.	(a)	In AH Processing not all the fields in an IP header are included in MAC Calculation. For each of the fields in the IPv4 header, indicate whether the filed is immutable, mutable but predictable, or mutable(zeroed prior to ICV calculation). a) Do the same for IPv6 header b) Do the same for IPv6 extension headers. c) In this case, justify your decision for each field.	CO5- Ana	(20)
		Or		
	(b)	You are the network administrator for a company, and you have been tasked with securing the company's internal network from external threats while allowing necessary outbound traffic. Given the following requirements: Employees need to access the internet for web browsing, but should not be able to access social media sites during work hours. External users should not be able to initiate connections to the internal network, except for a public web server hosted internally. Certain internal systems should only communicate with specific external IP addresses for software updates. How would you configure the firewall rules to meet these requirements? Provide a step-by-step explanation of the rules you would set up, and explain the reasoning behind each rule. Discuss how each rule contributes to both security and functionality.	CO5- Ana	(20)
5.	(a)	Explain about Worm hole attack in wireless system.	CO2-U	(20)
		Or		
	(b)	Explain about security in Ad-hoc network.	CO2-U	(20)