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

Question Paper Code: U2304

M.E. DEGREE EXAMINATION, NOV 2024

Second Semester

Computer Science and Engineering

21PCS204 - NETWORK SECURITY

(Regulation 2021)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART A - (5 x 20 = 100 Marks)

1.	(a)	Explain classical Encryption techniques in detail.	CO1- U	(20)
		Or		
	(b)	Explain how network issues can be solved.	CO1- U	(20)
2.	(a)	Show that in DES the first 24 bits of each sub key come from the same subset of 28 bits of the initial key and that the second 24 bits of each sub key come from a disjoint subset of 28 bits of the initial key.	CO2- App	(20)
		Or		
	(b)	State and explain the principles of public key cryptography.	CO1- U	(20)
3.	(a)	Users A and B use the Diffie Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7. (i) If user A has private key XA=3.What is A's public key YA? (ii) If user B has private key XB=6 What is B's public key YB? (iii) What is the shared secret key? Also write the algorithm. (iv) How man in middle attack can be performed in Diffie Hellman algorithm.	CO1- U	(20)
		Or		
	(b)	How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components.	CO1- U	(20)

4.	(a)	User A and B use a Diffie - Hellman key Exchange technique a common prime p=1 and primitive root α=7 are used. X_A=5 what is $Y_{A?}$	CO2- App	(20)
		Or		
	(b)	Apply Secure Electronic Transaction for E-Banking Application for card holders purchase request and verification by the merchants.	CO2- App	(20)
5.	(a)	How can a user maintain the password? Explain the password management in detail	CO1- U	(20)
		Or		
	(b)	Define intrusion detection and the different types of detection mechanisms, in detail.	CO3- U	(20)