E **Reg. No. :** | | | | | | | | | | |

Question Paper Code: 55S09

M.E. DEGREE EXAMINATION, MAY 2018

First Semester

Communication Systems

15PCM509 COMMUNICATION NETWORK SECURITY

(Regulation 2015)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART - A (5 x 20 = 100 Marks)

1.	(a)	(i) Discuss any four Substitution Technique and list their merits and demerits.	CO1- U	(10)
		(ii) Explain in detail Transposition Technique.	CO1- U	(10)
		Or		
	(b)	(i) Briefly explain the design principles of block cipher.	CO1- U	(10)
		(ii) Discuss in detail block cipher modes of operation.	CO1- U	(10)
2.	(a)	(i) Explain the generation sub key and S Box from the given 32-bit key byBlowfish.	CO2- U	(10)
		(ii) In AES, hoe the encryption key is expanded to produce keys for the 10 rounds	CO2- U	(10)
		Or		
	(b)	(i) Explain the Miller-Rabin Algorithm	CO2- U	(10)
		(ii) Describe about RC4 algorithm.	CO2- U	(10)
3.	(a)	How man in middle attack can be performed in Diffie Hellman algorithm.	CO3- U	(20)
		Or		

	(b)	Describe the MD5 message digest algorithm with necessary block diagrams.	CO3- U	(20)
4.	(a)	How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components.	CO4- U	(10)
		Or		
	(b)	Explain the architecture of IP Security.	CO4- U	(20)
5.	(a)	(i) Explain any two approaches for intrusion detection.	CO-5 U	(10)
		(ii) Identify a few malicious programs that need a host program for their existence.	CO-5 U	(10)
		Or		
	(b)	Define intrusion detection and the different types of detection mechanisms, in detail.	CO-5 U	(20)