E **Reg. No. :** □□□□□□□□□□

Question Paper Code : 55Q09

M.E. DEGREE EXAMINATION, NOV 2019

Elective

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) Briefly explain the design principles of block cipher. CO1- U (10)

(ii) Discuss in detail block cipher modes of operation. CO1- U (10)

Or

(b) (i) Discuss any four Substitution Technique and list their merits and demerits. CO1- U (10)

(ii) Discuss in detail block cipher modes of operation. CO1- U (10)

2. (a) (i) Identify the possible threats for RSA algorithm and list their counter measures. CO2- U (10)

(ii) Draw the general structure of DES and explain the encryption decryption process. 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) (i) Write and explain the digital signature algorithm. CO3- U (10)

(ii) Explain in detail Hash Functions. CO3- U (10)

4. (a) Explain the architecture of IP Security. CO4- 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. CO4- U (20)

5. (a) Describe the familiar types of firewall configurations. CO5- U (20)

Or

(b) Explain the types of Host based intrusion detection. List any two IDS software available. CO5-U (20)