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

Question Paper Code: 52299

M.E. DEGREE EXAMINATION, NOV 2016

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) Discuss any four substitution technique and list their merits and demerits. (10)

(ii) Explain in detail transposition technique. (10)

Or

(b) (i) Briefly explain the design principles of block cipher. (10)

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

2. (a) Identify the possible threats for RSA algorithm and list their counter measures. (20)

Or

(b) (i) Describe about RC4 algorithm. (10)

(ii) Explain the Miller-Rabin algorithm. (10)

3. (a) (i) Write and explain the digital signature algorithm. (10)

(ii) Explain in detail Hash Functions. (10)

Or

(b) Describe the MD5 message digest algorithm with necessary block diagrams. (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. (20)

Or

(b) (i) What is Kerberos? Explain how it provides authenticated service. (10)

(ii) Explain the format of the X.509 certificate. (10)

5. (a) (i) Explain firewalls and how they prevent intrusions. (10)

(ii) List and Brief, the different generation of antivirus software. (10)

Or

(b) Describe the familiar types of firewall configurations. (20)