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

Question Paper Code: 92021

M.E. DEGREE EXAMINATION, OCTOBER 2014.

First Semester

Communication Systems

01PCM509 – COMMUNICATION NETWORK SECURITY

(Regulation 2013)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions.

PART A - (10 x 2 = 20 Marks)

1. Differentiate a threat and attack.
2. Define cryptanalysis.
3. Can a meet-in-the middle attack be possible on a DES encrypted text? Justify.
4. State any two major design constraints for a stream cipher.
5. Differentiate a session key and a master key.
6. In what order, the signature function and the confidentiality functions are applied to a message? Defend your answer.
7. Why does ESP include a padding field in IP security?
8. List the parameters that define an SSL session state.
9. State the issue of tunneling in wire lease network security.
10. Differentiate wired and wireless security.

PART - B (5 x 14 = 70 Marks)

11. (a) Categorize any four types of active attacks possible for an information base. Give suitable examples for each of them. Analyze the solutions for these attacks also. (14)

Or

(b) Devise a generic model for network security. Illustrated the features of various components present in this architecture. (14)

12. (a) List various steps involved in a single round of DES algorithm. Show how substitution and permutation happen here. (14)

Or

(b) (i) Using the given playfair matrix, encrypt the given message: Want to read a book on sensors immediately.

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

(7)

(ii) Decipher the encrypted message YITJP GWJOW using the hill cipher with the inverse key $\begin{pmatrix} 5 & 1 \\ 2 & 7 \end{pmatrix}$ (7)

13. (a) (i) Explain the requirements of HASH. How does MAC differ from HASH?

(7)

(ii) With schematic explain Digital signature. (7)

Or

(b) (i) On the elliptic curve over the real numbers $y^2=x^3-36x$, let P=(-3.5,9.5) and Q=n(-2.5,8.5). Find P+Q and 2P. (7)

(ii) Devise a pseudo code on Diffie- Hellman Key exchange process. (7)

14. (a) Present the generic format of IPSec ESP and discuss the significance of various fields present in it. Also, describe how ISAKMP/Oakley key management protocol works for IPsec. (14)

Or

(b) Elucidate the operating principles, pros and cons of packet filtering firewalls, applications level gateways and circuit-level gateways. (14)

15. (a) Explain any two mechanisms adopted to secure a static Wireless Sensor Networks. Analysis the characteristics of the network and the type of mechanism used. (14)

Or

(b) Brief the possible solution scenarios to handle Worm hole and DoS attacks for a wireless networks. (14)

PART - C (1 x 10 = 10 Marks)

16. (a) Illustrate various steps involved in SHA-512 algorithm. Trace the same with a suitable example. (10)

Or

(b) List various types and subtypes supported by MIME. Show how S/MIME processes certificates. (10)

———————