KUMARAGURU
college of technology
character is life

Register Number:……..….

M.E DEGREE EXAMINATIONS: NOV/DEC 2014

(Regulation 2013)

Third Semester

COMMUNICATION SYSTEMS

P13COTE07: Communication Network Security

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 2 = 20 Marks)

1. What are the components of network security model?
2. Use the Vigenere cipher with keyword ‘HEALTH’ to encipher the message ‘LIFE’.
3. The input /output relation in a 2x2 S box is shown by the following table. Show the table for the inverse s box.

		Input Right bit	
		0	1
Input left bit	0	01	11
	1	10	00

4. Enumerate the characteristics of Advance Encryption Standard.
5. In ECB mode, bit 17 in cipher text block 8 is corrupted during transmission .Find the possible corrupted bits in the plaintext.
6. Find the result using Fermat’s little theorem $5^{15} \bmod 13$.
7. State the significance of one way function used in ECC.
8. Define the criteria for a cryptographic hash function.
9. In Diffie Hellman protocol g=7,p=23,x=3 and y=5.What is the value of the symmetric key?
10. Mention the various phases of virus.

Answer any FIVE Questions:-

PART B (5 x 16 = 80 Marks)

Q.No:11 is Compulsory

11. (i) What is design objective of S-box and P-box in encryption algorithm? (6)

(ii) Use a hill cipher to encipher the message ‘blah’ .Use the following key (10)

$$\begin{pmatrix} 2 & 5 \\ 9 & 4 \end{pmatrix}$$ and also perform decryption.

12. (i) Discuss the design issues and principles of OSI security architecture. (10)

(ii) Compare symmetric and asymmetric encryption techniques. (6)

13. Draw the structure of AES algorithm. Explain its features and block cipher modes of operation.

14. (i) What are the approaches to produce message authentication? (6)

(ii) Explain RSA based digital signature standard. (10)

15. (i) What are the security attacks in WEB? Mention the key components of secure electronic transaction. (8)

(ii) Explain the services provided by SSL and TLS. (8)

16. Explain the design principles of firewall and demonstrate various phases of system security development life cycle.

****