Register Number: ……

M.E. DEGREE EXAMINATIONS: NOV/DEC 2010

Third Semester

COMMUNICATION SYSTEMS

COM516: Communication Network Security

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

Answer ALL Questions:-

PART A (10 x 2 = 20 Marks)

1. Compare active and passive attacks.
2. What are the essential ingredients of symmetric cipher?
3. What is the difference between shiftrows and rotword in AES?
4. What is the difference between link and end-to-end encryption?
5. Compare symmetric and public key encryptions.
6. What is the difference between MAC and Hash functions?
7. What four requirements are defined by Kerberos?
8. Define S/MIME?
9. List the 3 classes of intruders.
10. Define virus. Specify the types of viruses.

PART B (5 x 16 = 80 Marks)

11. a) Explain the various security services and security mechanisms defined in X.800.

(OR)

b) (i)Explain in detail about DES Encryption Algorithm. (12)

(ii) Encrypt the message “youcanwin” using Playfair cipher with keyword “APPLE” (4)

12. a) Explain in detail about AES Encryption Algorithm.

(OR)

b) Explain the following

(i) RC4 stream cipher (8)

(ii) Key distribution scenario in symmetric Encryption (8)

13. a) (i) Explain in detail about RSA algorithm using one example. (10)

(ii) Users A and B use the Diffie-Hellman encryption algorithm with a common prime q = 71 and a primitive root α=7. User A and B have private keys X_A = 5 and X_B =12 respectively. Find out A's public key, B's public key and the shared secret key. (6)

(OR)

b) Explain the various Digital Signature approaches and algorithm in detail.

14. a) (i) Explain in detail about Kerberos Version 4 Message Exchange. (12)

(ii) Mention the Environmental shortcomings of Kerberos version 4 over version 5. (4)

(OR)

b) (i) Discuss in detail about the various services provided by PGP (PRETTY GOOD PRIVACY).

15. a) Explain in detail about the various types of firewalls.

(OR)

b) (i)Explain the two approaches of Intrusion detections. (12)

(ii) Discuss about the four strategies used for password selection. (4)

****