LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

M.Sc. DEGREE EXAMINATION – COMPUTER SCIENCE

SECOND SEMESTER – APRIL 2010

CS 2813 - CRYPTOGRAPHY & NETWORK SECURITY

Date & Time: 21/04/2010 / 1:00 - 4:00 Dept. No. Max. : 100 Marks

SECTION-A

ANSWER ALL THE QUESTIONS: (10 x 2 = 20)

1. What is peer entity authentication?
2. Give the encryption and decryption technique of Caesar Cipher.
3. Differentiate block cipher and stream cipher.
4. Enumerate the differences between link encryption and end to end encryption.
5. What is digital signature?
6. What is MAC?
7. What is S/MIME?
8. Name any four IPSec Services.
9. What is a Trap Door?
10. What is Base Rate Fallacy?

SECTION-B

ANSWER ALL THE QUESTIONS: **(5 x 8 =40)**

11. a) Give an overall view of the Simplified DES with its encryption and decryption.

(OR)

b) Explain briefly transposition techniques.

12. a) Explain briefly Blowfish's encryption and decryption with a neat diagram.

(OR)

b) Explain RSA Algorithm with respect to Public Key Cryptography.

13. a) What is hashing and explain briefly MD5.

(OR)

b) Explain the different methods of distributing the public keys.

14. a) Explain in brief the applications and benefits of IPSec.

(OR)

b) Discuss briefly about the Kerberos.

15. a) Explain in brief the four strategies for password selection.

(OR)

b) Discuss about the characteristics of Bastion Host.

SECTION-C

ANSWER ANY TWO QUESTIONS: (2 x 20 = 40)

16. (a) What is OSI Security Architecture? Explain the mechanisms of OSI Security Architecture in detail. (10)
    (b) Discuss about the characteristics of advanced symmetric block ciphers by comparing the different block ciphers. (10)

17. (a) Explain Key Management and Diffie Hellman Key Exchange with a neat diagram. (10)
    (b) Discuss in detail about the SSL Architecture. (10)

18. (a) Draw and explain the types of firewall. (10)
    (b) Discuss in detail the two approaches of intrusion detection. (10)

****