LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

M.Sc. DEGREE EXAMINATION – **COMPUTER SCIENCE**

SECOND SEMESTER – **APRIL 2014**

CS 2817/2823 - CRYPTOGRAPHY & NETWORK SECURITY

Date : 28/03/2014 Dept. No. Max. : 100 Marks
Time : 09:00-12:00

SECTION-A

ANSWER ALL THE QUESTIONS: **(10 X 2 = 20)**

1. Compare a threat and an attack.
2. What are transposition techniques?
3. Differentiate block cipher and stream cipher.
4. What is asymmetric encryption?
5. Define: Authenticator.
6. Expand DSA and state its purpose.
7. Enumerate any two benefits of IPSec.
8. Mention the message format of SSL Change Cipher Spec Protocol and its purpose.
9. Mention the three classes of intruders.
10. What is Zombie?

SECTION-B

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

11. a) Explain about the security services in OSI Security architecture.

(OR)

b) Elaborate Playfair Cipher and the rules for encryption with an example.

12. a) Explain in brief the operations involved in Blowfish.

(OR)

b) Discuss about the characteristics of advanced symmetric block ciphers.

13. a) Discuss in brief about digital signatures.

(OR)

b) Explain the steps involved in MD5 Message Digest Algorithm.

14. a) Discuss about the features of S/MIME.

(OR)

b) Describe the salient features of KERBEROS.

15. a) Explain the following: (a) Honey Pots (b) Logic Bomb

(OR)

b) Explain the different strategies for selecting passwords.

SECTION-C

ANSWER ANY TWO QUESTIONS: **(2 X 20 = 40)**

16. (a) Discuss in detail about the encryption and decryption techniques involved in Simplified DES. (10)

    (b) Explain RC4 in detail with a neat diagram of its encryption and decryption. (10)

17. (a) What is Key Management and elaborate the steps involved in Diffie Hellman Key Exchange. (10)

    (b) Discuss in detail about the IP Security Architecture. (10)

18. (a) Explain the two different approaches of Intrusion Detection Systems. (10)

    (b) Discuss about the three different types of protocols in SSL Architecture. (10)

****