 LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

 **M.Sc.** DEGREE EXAMINATION - **COMPUTER SC.**

SECOND SEMESTER – APRIL 2012

# CS 2813 - CRYPTOGRAPHY & NETWORK SECURITY

 Date : 21-04-2012 Dept. No. Max. : 100 Marks

 Time : 9:00 - 12:00

**SECTION-A**

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

1. Write down the format of initial permutation of DES.
2. Define substitution and Transposition Methods.
3. Define prime number
4. What is RC5-CTS mode?
5. What is one way property of hash function?
6. What are time stamps?
7. What is S/MIME?
8. What is handshake protocol?
9. Write down the phases of Virus
10. What is misfeasor?

**SECTION-B**

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

1. a) Explain Poly Alphabetic Cipher with an example

(OR)

 b) Explain Play fair Cipher technique with an example

 12. a) Explain RSA algorithm.

 (OR)

 b) Explain the key distribution Scenario.

 13. a) Explain approaches of digital signature standard

 (OR)

 b) Write down the requirements for a hash function.

 14. a) Explain MIME content types.

 (OR)

 b) Explain SSL record protocol

 15. a) Explain rule based Intrusion Detection.

 (OR)

 b)Explain the password selection strategies.

**SECTION-C**

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

16. i) Explain Hill Cipher and find the cipher text of “POT” using

 17 17 5 4 9 15

 K= 21 18 21 and K-1 = 15 17 6

 2 2 19 24 0 17

 ii) Explain RC5 algorithm in detail.

17. i) Explain SHA algorithm in detail.

 ii) Explain IPSec Architecture in detail.

18. i) Explain different types viruses.

 ii) Explain Digital Signature standard

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*