LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

SECOND SEMESTER – **APRIL 2019**

CS 2817– CRYPTOGRAPHY & NETWORK SECURITY

Date: 13-04-2019 Dept. No. □ Max. : 100 Marks

Time: 09:00-12:00

PART A **(4 x 10=40 marks)**

Answer any four questions:

1. Differentiate active and passive attacks. Explain the three key objectives of computer security.
2. What are substitution techniques? Explain any twowith example.
3. Define symmetric encryption. Differentiate block cipher and stream cipher design principles.
4. Perform encryption for the plain text M = 88 using the RSA Algorithm p = 17, q = 11 and the public component e =7 .
5. What is meant by IP Security? Write the applications and benefitsof IPsec.
6. Write short notes on S/MIME messages and its content types.
7. Define Virus. Write short notes on the types of viruses.
8. Explain the concept of trusted systems with reference monitor concept.

PART B **(3x20=60 marks)**

Answer any three questions:

9. a) Explain OSI security architecture in detail.

   b) Explain DES encryption algorithm with general diagram.

10. a) Explain the basic key management methods with example.

    b) Explain any two transposition encryption techniques with examples.

11. a) With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than 2^{128}bits and produces an output of 512-bit message digest.

    b) Briefly explain RC4 stream cipher algorithm with example.

12. a) Explain transport layer security using pseudorandom function.

    b) Explain Diffie-Hellman key exchange algorithm with one simple example.

13. a)Give the general model of digital signature process.(5 Marks)

    b) Mention the significance of signature function in Digital Signature Standard (DSS) approach.(15 Marks)

14. a)What are the classification of intruders? Explain any two intrusion detection techniques.

    b) Briefly explain password management in Network Security.

★★★★★★★