LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

THIRD SEMESTER – **NOVEMBER 2019**

18PCS3MC04 – CRYPTOGRAPHY AND CYBER SECURITY

Date: 02-11-2019 Dept. No. □ Max. : 100 Marks
Time: 09:00-12:00

PART A (10x2=20 Marks)

Answer all the questions:

1. What are the three key objectives of computer security?
2. What is the difference between passive and active security threats?
3. What are the two general approaches used to attack a conventional encryption scheme?
4. Define symmetric encryption.
5. Define cryptographic hash function.
6. Give the general model of digital signature process.
7. What are the classification of intruders?
8. Define Computer Virus.
9. Define computer Ethics.
10. List any four computer crimes.

PART B (5x8=40 Marks)

Answer all the questions:

11 a). Explain the model of network security with diagram.

OR

b) What are substitution techniques. Give two examples.

12. a). Explain the steps of RC4 stream cipher algorithm.

OR

b) Explain triple DES and meet-in-middle attack.

13. 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 as output a 512-bit message digest.

OR

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

14. a). Explain any two intrusion detection techniques.

OR

b). Explain the phases of virus and types of viruses.

15 a). Briefly explain the types of computer crimes.

OR

b). Explain the laws, investigation and ethics for information security.

PART C **(2x20=40 Marks)**

Answer any two questions:

16. a) Explain OSI security architecture in detail.

b) Explain RSA algorithm. Perform encryption of plain text M = 88 using p = 17, q = 11 and e =7.

17.a) What are the applications of cryptographic Hash functions. Explain each with a neat diagram.

b) Briefly explain firewall design principles, characteristics and its types.

18.a) Briefly explain computer forensics and issues of computer forensics.

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

-------$$$$$-----