LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

THIRD SEMESTER – **NOVEMBER 2018**

16/17PCS3MC04 – CRYPTOGRAPHY AND CYBER SECURITY

Date: 29-10-2018 Dept. No. Max. : 100 Marks

Time: 09:00-12:00

PART A (10x2=20 marks)

Answer all the questions:

1. Write any four security mechanisms.
2. What is the difference between passive and active security threats?
3. Define Brute-force attack.
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 Virus.
9. Define computer Ethics.
10. List any four computer laws.

PART B (5x8=40 marks)

Answer all the questions:

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

OR

b) What are substitution cipher techniques? Give two examples.

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

OR

b) Explain the steps of RSA algorithm with example

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 in detail.

OR

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

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

OR

b). Explain the investigation process and ethics for information security.

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

Answer any two questions:

16. a) Explain OSI security architecture in detail.

b) Differentiate block cipher and stream cipher design principles. Explain DES encryption algorithm with general diagram.

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

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

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

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

$$$$$$$$