LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

THIRD SEMESTER – **NOVEMBER 2022**

PCS 3504 – CRYPTOGRAPHY AND CYBER SECURITY

Date: 28-11-2022 Dept. No. Max. : 100 Marks

Time: 09:00 AM - 12:00 NOON

PART - A

Answer ALL the questions: **(10x2=20 marks)**

1. List the key objectives of computer security.
2. Differentiate Active and Passive attacks.
3. What are the types of attack on an encryption algorithm?
4. What is Steganography?
5. Define cryptographic hash function.
6. Give the general model of digital signature process.
7. What are the classification of intruders?
8. Define Virus and Worms.
9. Define computer Ethics.
10. List any four computer related laws.

PART - B

Answer ALL the questions: **(5x8=40 marks)**

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

(OR)

b) Define briefly about playfair cipher and ceaser cipher.

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

(OR)

b) Explain any two pseudo random number generator algorithms.

13. a) With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message and produces 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 techniques used on password management in detail.

PART - C

Answer any TWO questions: **(2x20=40 marks)**

16. a) Explain OSI security architecture in detail.

    b) Explain DES algorithm with key generation and block diagram of single round.

17. a) Explain the applications of cryptographic hash functions with necessary diagrams.

    b) What are the various types of firewalls? Explain each of them in detail.

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

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

$$$$$$$