LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

THIRD SEMESTER – **NOVEMBER 2023**

PCS 3504 – CRYPTOGRAPHY AND CYBER SECURITY

Date: 07-11-2023 Dept. No. Max. : 100 Marks

Time: 01:00 PM - 04:00 PM

PART A

Answer all the questions: **(10x2=20)**

1. Differentiate active and passive attacks.
2. Define computer security.
3. What are the types of attack on an encryption algorithm?
4. What is Steganography?
5. Define cryptographic hash function.
6. What are the applications of cryptographic hash functions?
7. List the three classes of intruders.
8. Define Virus. Write the types of viruses.
9. What are the types of intellectual property?
10. What is computer forensics?

PART B

Answer all the questions **(5x8=40)**

11 a) What are substitution techniques. Give two examples.

OR

b) Explain the model of network security with diagram.

12. a). Perform encryption for the plain text M = 2 using the RSA Algorithm, p = 3, q = 11 and the public component e =7.

OR

b) What are pseudo random number generator algorithms? Explain in detail.

13. a) Explain Diffie –Hellman key exchange algorithm with simple example.

OR

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

14. a). Explain the various intrusion detection techniques.

OR

b). Explain password management in detail.

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

OR

b). Discuss the investigation steps and the branches of digital forensics.

PART C

Answer any two questions **(2x20=40)**

16. a) Explain the OSI security architecture in detail.

b) Explain DES encryption algorithm with general diagram.

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

b) What are the various types of firewalls? Explain any two in detail.

18. a) Briefly explain the laws, investigation and ethics of computer information security.

b) Define briefly about play fair cipher and encrypt the text “MOVE FORWARD” Using key “MONARCHY”.

&&&&&&&&&&