LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

THIRD SEMESTER – **APRIL 2023**

PCS 3504 – CRYPTOGRAPHY AND CYBER SECURITY

Date: 08-05-2023 Dept. No. Max. : 100 Marks
Time: 09:00 AM - 12:00 NOON

PART A (10x2=20 marks)

Answer ALL the questions:

1. Differentiate active and passive attacks.
2. Define computer security.
3. Differentiate block cipher and stream cipher.
4. What is TRNG?
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. List any four computer related laws.

PART B

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

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

OR

b) Write the Euclidean Algorithm to find the GCD of two numbers.

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) What is computer forensics? Write the steps of computer forensics.

PART C

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

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

b) Explain DES encryption algorithm with general diagram.

17. a) Explain the steps of RC4 stream cipher algorithm with neat diagram.

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

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

b) Explain message authentication and digital signatures with necessary diagrams.

$$$$$$$