 **ST. JOSEPH’S UNIVERSITY, BANGALORE -27**

Register Number:

Date: 10-12-2022 ( 1PM)

**M.SC I SEMESTER**

**SEMESTER EXAMINATION: December 2022**

(Examination conducted October 2022)

**CS 7421– CYBER SECURITY**

**Time: 2Hrs. Max Marks - 50**

 **This Paper question paper contains 2 printed pages and three parts**

**Part A**

**I Answer all the following 1\*5= 5**

1. Define Stream Cipher with an example.
2. Describe CBC in a Block Cipher scheme.
3. What is a honeypot?
4. Differentiate between Authorization and Authentication
5. What are the four most common digital forensics Investigation Process?

**Part B**

**II Answer Any Five of the following 3 \* 5= 15**

1. List the Five ingredients of a typical Conventional Encryption Model.
2. What is the difference between differential and linear cryptanalysis?
3. Discuss Secure Socket Layer with a suitable diagram.
4. Explain the three common types of firewalls.
5. Define Message Authentication and write its two cryptographic techniques.
6. Give any 3 preventive measures against phishing attacks.
7. Distinguish between Trojan horse and Worm as a computer virus/ malware.

**Part C**

**III. Answer any three of the Following 10\* 3= 30**

1. a) Distinguish between Pretty Good Privacy and Secure/Multipurpose Internet Mail Extension (4 marks)

b) How we can encrypt plaintext 9 using the RSA public-key encryption algorithm. This example uses prime numbers 7 and 11 to generate the public and private keys.

 (6 marks)

1. a) Why is an Antivirus important? List four virus counter measures (4 marks)

 b) Illustrate a simple distributed SYN Flood Attack with a suitable diagram (6 marks)

1. a) Explain the significance of ISO? Mention any common cyber standards. (3 marks)

b) Explain DES algorithm and mention its strengths (7 Marks)

 16 a) Elaborate on digital Forensics process (4 Marks)

 b) What are the most potent threats to the safety and sovereignty of Indian cyber space? What are the recent measures to strengthen the security of Indian cyber space ? Examine.

 (6 Marks)