(3 Hours) **[Total Marks: 80]**

N.B. (1) Question No. **1** is **Compulsory.**
(2) Attempt any **three** questions from the remaining **five** questions.
(3) Answers to **sub-questions** should be **grouped** and written **together.**

Q1.	**Answer ANY FOUR out of FIVE questions.**	**20**
A.	Explain a global perspective on cybercrime.	
B.	Explain - Cyber bullying	
C.	How can keyloggers be used to commit cybercrime?	
D.	What is chain of custody?	
E.	What is digital evidence?	
Q2. A	Explain Social engineering? Explain precautions to be taken against social engineering attack.	**10**
Q2. B	Describe the general procedure for collecting digital evidence from a crime scene.	**10**
Q3. A	Discuss the various categories of steganography with examples.	**10**
Q3. B	Illustrate Digital Forensic life cycle with diagram.	**10**
Q4. A	Explain the steps involved in email communication and how forensic experts use IP tracking.	**10**
Q4. B	Discuss the types of phishing attacks and the best practices to prevent them.	**10**
Q5. A	What is an intrusion detection system? Explain in detail different types of intrusion detection systems.	**10**
Q5. B	Discuss significance of data recovery in digital forensics and business continuity.	**10**
Q6. A	How do the criminals plan the attacks?	**10**
Q6. B	What are the key provisions of the Indian IT Act, 2000 and their impacts in dealing with cybercrimes in India?	**10**

X525Y9C9719X525Y9C9719X525Y9C9719X525Y9C9719