(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.**

Q.1	(a)	What are the key provisions in the Indian ITA - 2000?	5
	(b)	Explain the concept of Antiforensics.	5
	(c)	What is digital evidence? What are the characteristics of good evidence?	5
	(d)	Explain the role of an intrusion detection system in network security.	5
Q.2	(a)	Explain the different types of phishing attacks. What steps can be taken to avoid phishing attacks?	10
	(b)	Explain the concept of duplication and preservation of digital evidence in detail.	10
Q.3	(a)	Explain the various types and techniques of credit card fraud. How can it be prevented?	10
	(b)	What is steganography? Discuss the different categories of steganography.	10
Q.4	(a)	Explain various phases and activities involved in the life cycle of a forensics investigation process.	10
	(b)	Explain the classifications of cybercrime with suitable examples.	10
Q.5	(a)	How does a buffer overflow occur? What measures can be taken to prevent buffer overflow vulnerabilities?	10
	(b)	Explain in detail how cybercriminals plan and execute attacks.	10
Q.6	(a)	What are the different e-mail protocols? Explain how an e-mail can be traced for forensics purpose.	10
	(b)	What is data recovery? Explain the role of backup in data recovery.	10