

Duration: 3 hours

Max. Marks: 80

- N.B.:** 1) Question No.1 is **compulsory**.
2) Attempt any **THREE** questions out of remaining **FIVE** questions.
3) **Figures** to the **right** indicates **full** marks.
4) Assume suitable data if **necessary**.

- Q1 Attempt any FOUR of the following 20**
- a List General guidelines for password policies.
 - b Difference between virus and worm.
 - c How cybercrimes differs from most terrestrial crimes?
 - d What are different Security Risks for Organizations?
 - e What are Mobile Vulnerabilities?
- Q.2 10**
- a Discuss steps involved in planning of cyberattacks by criminal. **10**
 - b What is vishing attack? How it works? How to protect from vishing attack? **10**
- Q.3 10**
- a What is e-commerce? Discuss types of e-commerce. **10**
 - b Explain E-contracts and its different types. **10**
- Q.4 10**
- a What are basic security precautions to be taken to safeguard Laptops and Wireless devices? Explain. **10**
 - b What is Cybercrime? Who are Cybercriminals? Explain. **10**
- Q.5 10**
- a What is digital evidence? Where one can find it. **10**
 - b What are illegal activities observed in Cyber Cafe? What are safety and security measures while using the computer in Cyber Cafe? **10**
- Q.6 Write short notes on any FOUR 20**
- a Cyberdefamation
 - b HIPAA
 - c Buffer overflow attack
 - d Steganography
 - e DDOS attack
 - f Trojan horse and backdoor
