Seat No.: _____ Enrolment No._____

# GUJARAT TECHNOLOGICAL UNIVERSITY

**M.C.A.- SEMESTER – V • EXAMINATION – WINTER 2012**

**Subject code: 650008 Date: 28-12-2012**

**Subject Name: Cyber Security and Forensics (CSF)**

**Time: 10:30 am – 1:00 pm Total Marks: 70**

## Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

| | | | |
|---|---|---|---|
| **Q.1** | **(a)** | Define the following terms :<br>1. Cybercrime 2. Social Engineering<br>3. Active Attack 4. Trojan Horse<br>5. Whaling 6. Digital Forensics<br>7. LDAP | **07** |
| | **(b)** | How do we classify cybercriminals? Explain cybercrime against organization briefly. | **07** |
| **Q.2** | **(a)** | What kinds of attacks are possible on mobile/cell phones? Explain each one briefly. | **07** |
| | **(b)** | i. Explain how Botnets can be used as a fuel to cybercrime.<br>ii. Explain types of services provided by cloud computing. | **04**<br>**03** |
| | | **OR** | |
| | **(b)** | i. What is cyberstalking? What are the types of stalkers? Provide Example.<br>ii. Prepare security guidelines which can be implemented in an organization. | **04**<br>**03** |
| **Q.3** | **(a)** | Explain the various measures for protection of laptops through physical measures and logical access control measures. | **07** |
| | **(b)** | What are the different phases during the attack on the network? | **07** |
| | | **OR** | |
| **Q.3** | **(a)** | How Computer virus can be categorized? Explain each. | **07** |
| | **(b)** | What is DoS attack? List and Explain classification and levels of DoS attack? | **07** |
| **Q.4** | **(a)** | i. What are the different methods of Phishing?<br>ii. What are Spam and Hoax E-Mails? | **04**<br>**03** |
| | **(b)** | Under the Indian IT Act, is there a legal protection available for “personal data” or “sensitive personal data”? Explain how. | **07** |
| | | **OR** | |
| **Q.4** | **(a)** | What is Identity Theft? What are types of Identity Theft? Explain each. | **07** |
| **Q.4** | **(b)** | i. Do “electronic records” have the admissibility into Indian Courts? Explain why.<br>ii. What is the meaning of “cyberlaw”? Explain the concept of “trust seal”. | **04**<br>**03** |
| **Q.5** | **(a)** | i. What is computer forensics? Explain how the “chain of custody” concept applies in computer/digital forensics.<br>ii. Explain why the NDA is important in a forensics investigation? List and explain Elements of forensics investigation contract. | **04**<br>**03** |
| | **(b)** | What are the various phases and activities involved in the life cycle of a forensics investigation process? | **07** |
| | | **OR** | |
| **Q.5** | **(a)** | i. What are rootkits? Why are they dangerous? How do rootkits help cyberattckers?<br>ii. Provide an overview of how “data mining” techniques can be applied in cyberforensics. | **04**<br>**03** |
| | **(b)** | Explain forensics examination of PDAs and iPhones. | **07** |

**********