Seat No:_____ Enrollment No:_____

PARUL UNIVERSITY

FACULTY OF IT & COMPUTER SCIENCE

MCA/IMCA Summer 2018- 19 Examination

Semester: 4/8 **Date: 22/04/2019**
Subject Code: 05201284/05301484 **Time: 2:00pm to 4:30pm**
Subject Name: Information Security and Cyber Forensics **Total Marks: 60**

Instructions:
1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Make suitable assumptions wherever necessary.
4. Start new question on new page.

Q.1 Answer the followings.

A. Answer in short. **(05)**

1. Define information security.
2. What is security threat?
3. What is computer forensics?
4. What is Forensic SIM?
5. What is Phishing?

B. Multiple choice type questions/ Give the sentence true or false. (Each of 01 marks) **(10)**

1. In Active attack data will not be altered – true or false
2. Security threat frequency is part of Hybrid model for threat classification: True or false
3. Authentication is a process to revoke authority from users
4. Firewalls exist as hardware only: true or false
5. BYOD ("Bring Your Own Device") policy allows employees to integrate themselves more fully into their job: True or false
6. Acquisition is one of the process of forensic process : True or False
7. SSE stands for _____
   a. System Security Engineering
   b. System scrutiny Estimate
   c. System Software Estimation
   d. System Software Engineering
8. WPA stands for _____
   a. Wifi Protected Authentication
   b. Wifi Provider Access
   c. Wifi Protected Access
   d. Wifi Productive Access
9. DSSS stands for
   a. Direct-sequence spread spectrum
   b. Direct selective spread spectrum
   c. Direct spread sequence spectrum
   d. Direct Software selective spectrum
10. AES stands for
    a. Active Encryption standard
    b. Advanced Encryption Standard
    c. Advanced Elective Standards
    d. Adaptive Encryption Standard

Q.2 Answer the followings. (3 Mark Questions – Any Five) **(15)**

1. Describe Chain of custody.
2. Describe Technical challenges of digital forensic.
3. Describe different types of security threats
4. Describe Anti-forensic with its tool and techniques.
5. Describe patched operating in detail.
6. Describe Memory Protection technique.

Q.3 Answer the following. (Any three) **(15)**

1. Explain Operating system security with threat and trust models.
2. Explain attacks on Wireless network in detail
3. Write two case studies on virus attack.
4. Explain Task performed by Computer Forensics Tools in detail

Q.4 Answer the following.

A. Explain Forensic Auditing in details. **(05)**

B. Write a short note on WLAN standards with its signal transmission techniques **(10)**

OR

B. Write a short note on basic security principles for information systems development and deployment **(10)**