Roll No. | | | | | | | | | | |

Total No. of Pages : 02

Total No. of Questions : 09

MCA (Sem.–2)

INFORMATION SECURITY AND CYBER LAW

Subject Code : PGCA-1932

M.Code : 79619

Date of Examination : 14-07-22

Time : 3 Hrs.

Max. Marks : 70

INSTRUCTIONS TO CANDIDATES :

1. **SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.**
2. **SECTION - B & C have FOUR questions each.**
3. **Attempt any FIVE questions from SECTION B & C carrying TEN marks each.**
4. **Select atleast TWO questions from SECTION - B & C.**

SECTION-A

1. **Write short notes on :**

   a) Define any two components of Information Security.

   b) Define CIA triad.

   c) How is Biometric Authentication different from password authentication?

   d) Differentiate between Honeypots and Firewall?

   e) Differentiate between Virus and Trojans?

   f) What is the difference between Law and Ethics?

   g) Define digital signatures.

   h) What is the significance of honeypots?

   i) What is intellectual property?

   j) What is phishing?

SECTION-B

2. a. Differentiate between Password based and Token-based Authentication with suitable examples.

   b. Why and how to provide security to Database Management Systems?

3. Discuss and compare various access control policies.

4. What are the types of malicious software? How they harm the network system?

5. What is the need for database security? What are database access controls in Database Management System?

SECTION-C

6. What is Intrusion Detection System? Differentiate between Host based and Network based IDS?

7. Discuss about Indian Cyber Laws.

8. Define firewalls. What are the various types of firewalls?

9. Differentiate between symmetric and asymmetric encryption. Describe transposition techniques by taking suitable examples.

NOTE : Disclosure of Identity by writing Mobile No. or Marking of passing request on any paper of Answer Sheet will lead to UMC against the Student.

Roll No. | | | | | | | | | | | | Total No. of Pages : 02

Total No. of Questions : 09

MCA (Sem.–2)

INFORMATION SECURITY AND CYBER LAW

Subject Code : PGCA-1932

M.Code : 79619

Date of Examination : 30-11-2023

Time : 3 Hrs. Max. Marks : 70

INSTRUCTIONS TO CANDIDATES :

1. **SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.**
2. **SECTION - B & C have FOUR questions each.**
3. **Attempt any FIVE questions from SECTION B & C carrying TEN marks each.**
4. **Select atleast TWO questions from SECTION - B & C.**

SECTION-A

1. **Write short notes on :**

   a) What is the purpose of a firewall in network security?

   b) What are the three fundamental principles of information security represented by the acronym CIA?

   c) What role do security functional requirements play in the development of secure software and systems?

   d) What are the different types of user authentication methods commonly used in information security?

   e) What are the common security issues associated with password-based authentication methods?

   f) Explain the main security challenges in securing a database.

   g) Define the terms "worms" in the context of malicious software.

   h) Define the terms "trojans" in the context of malicious software.

   i) What are the primary functions of an Intrusion Detection System (IDS)?

   j) What are cyber laws, and how do they address legal issues related to the internet and information security?

SECTION-B

2. Describe the potential impact of a keylogger on a user's security and privacy.

3. What role do cryptographic algorithms play in ensuring the confidentiality and integrity of data?

4. What is the role of access control in information security and how can it be implemented to protect sensitive data?

5. How do security functional requirements help ensure that software and systems are secure and can you provide an example of one such requirement?

SECTION-C

6. How does an Intrusion Prevention System (IPS) differ from an IDS and why is it valuable in network security?

7. Discuss the key provisions in Indian cyber laws for the investigation and prosecution of cybercrimes.

8. Explain the primary objectives of a firewall in the context of network security. What are the main types of firewalls and how do they operate?

9. What are the key features and purposes of SSL and TLS in ensuring secure communication over the internet? How do they differ and which is more commonly used today?

NOTE : Disclosure of Identity by writing Mobile No. or Marking of passing request on any paper of Answer Sheet will lead to UMC against the Student.

Roll No. ☐☐☐☐☐☐☐☐☐☐ Total No. of Pages : 02

Total No. of Questions : 09

MCA (Sem–2)

INFORMATION SECURITY AND CYBER LAW

Subject Code : PGCA1932

M.Code : 79619

Date of Examination : 22-05-2024

Time : 3 Hrs. Max. Marks : 70

INSTRUCTIONS TO CANDIDATES :

1. SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.
2. SECTION - B & C have FOUR questions each.
3. Attempt any FIVE questions from SECTION - B & C carrying TEN marks each.
4. Select atleast TWO questions from SECTION - B & C.

SECTION-A

1. Write short notes on :

   a. What is a firewall in information security?

   b. What is an intrusion detection system in information security?

   c. What is penetration testing in information security?

   d. What is cyber law?

   e. What is a cyber crime?

   f. What is cyber stalking?

   g. What is identity theft?

   h. What is hacking?

   i. What is phishing?

   j. What is malware?

SECTION-B

2. What are some common threats to database security, such as unauthorized access, SQL injection attacks, and data leakage, and how can they be prevented or mitigated? What are some best practices for securing databases, such as access control, encryption, and data masking, and how can they be implemented in different types of database systems?

3. What are some common threats to each aspect of the CIA triad, and how can they be prevented or mitigated? How can organizations balance the need for security with the need for accessibility and usability of their data?

4. What is Role-Based Access Control (RBAC) in information security, and how does it help organizations manage access to their resources based on job functions and responsibilities? How is RBAC different from other access control models, such as Discretionary Access Control (DAC) and Mandatory Access Control (MAC)?

5. What are Denial-Of-Service (DoS) attacks and rootkits in information security, and how do they work to disrupt or compromise the availability, integrity, and confidentiality of data and systems? What are some common types of DoS attacks, such as flooding, amplification, and distributed DoS (DDoS), and how can they be prevented or mitigated?

SECTION-C

6. What is the role of IDS in detecting potential security breaches, and what are the different types of IDS used to monitor network traffic and system activity? What are some best practices for implementing a firewall and IDS in an organization, and how can they be used together to improve overall security posture?

7. What are cryptographic algorithms, and how are they used in information security to protect data confidentiality, integrity, and authenticity? What are the different types of cryptographic algorithms, and what are their strengths and weaknesses?

8. How can security policies be effectively communicated and enforced throughout an organization, and what are some best practices for maintaining and updating security policies over time? What are some examples of cyber laws and regulations, and how do they impact information security practices in different industries and jurisdictions?

9. What are some commonly used internet security protocols and standards, such as SSL/TLS, IPsec, and DNSSEC, and how do they help to secure communication and data exchange over the internet? How do these protocols and standards work to provide confidentiality, integrity, and authenticity of information, and what are some best practices for implementing them in an organization?

NOTE : Disclosure of Identity by writing Mobile No. or Marking of passing request on any paper of Answer Sheet will lead to UMC against the Student