MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
*(A constituent unit of MAHE, Manipal)*

**DEPARTMENT OF MECHATRONICS**

**VI SEMESTER B.TECH. (MECHATRONICS)**

**END SEMESTER EXAMINATION (REGULAR)**

SUBJECT: Information Security for Industrial Automation Subject Code: MTE 4056

**Date: 08/05/2024**

**Time: 3 Hrs** **Exam Time: 2:30PM – 5:30PM** **MAX. MARKS: 50**

Name: ……, Registration No: ……...

- Answer **ALL** the questions.

| Q. No. | Questions | M | CO | PO | LO | BL |
|---|---|---|---|---|---|---|
| **1A** | Adapt the proposed hacking topology strategy to better balance the goals of maximizing impact on selected victims while minimizing the risk of detection, within the ethical boundaries of authorized penetration testing. | **5** | **4** | **3** | **5** | **6** |
| **1B** | Analyze the four general techniques used by firewalls to control access and implement a site's security policy. | **3** | **3** | **2** | **2** | **4** |
| **1C** | Use Vigenère cipher, generate the ciphertext when the plaintext is "MAHEANINSTITUTIONOFEMINENCE", and the key is "MANIPAL." | **2** | **1** | **1** | **1** | **3** |
| **2A** | Evaluate the effectiveness of first-generation antivirus scanners compared to second-generation heuristic scanners in detecting and combating viruses. Consider factors such as their reliance on virus signatures, ability to detect unknown viruses, and approaches to identifying and removing infections. Support your evaluation with examples from the provided descriptions of both generations of antivirus software. | **4** | **2** | **2** | **2, 9** | **5** |
| **2B** | Apply Radix 64 conversion in Pretty Good Privacy (PGP) services to encrypt a plaintext message and generate a corresponding digital signature. | **4** | **3** | **5** | **3** | **3** |
| **2C** | Create a cryptographic system that ensures both confidentiality and authenticity, where the authentication mechanism is tied to the ciphertext. The authentication function should incorporate either a MAC algorithm or a SHA hash algorithm for authentication purposes. | **2** | **5** | **3** | **5** | **6** |
| **3A** | Evaluate the significance of the multipart content type in MIME (Multipurpose Internet Mail Extension) in terms of its ability to handle multiple independent body parts within an email | **4** | **3** | **5** | **3** | **5** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | message. Compare and contrast the use of multipart/mixed, multipart/parallel, multipart/alternative, and multipart/digest subtypes, discussing their respective functionalities and typical use cases. | | | | | |
| **3B** | Apply the concept of network intrusion detection systems to a scenario where an organization wants to protect its network from potential cyber threats. Describe how analyzing the frequency of specific network events could be utilized in this context. | **3** | **2** | **5** | **3** | **3** |
| **3C** | Dealing with the rising tide of cybercrimes, compare prevention and detection strategies in their approaches to addressing cybercrimes. | **3** | **4** | **2** | **2** | **4** |
| **4A** | Analyzing the mechanisms behind a SQL Injection Attack, identify and describe two key steps in the process, detailing how attackers exploit vulnerabilities in the query's input form. | **4** | **3** | **2** | **2, 3** | **4** |
| **4B** | Evaluate the effectiveness of the two-phase update approach proposed by Lampson and Sturgis for ensuring reliability and integrity in database management systems. Highlight the advantages and limitations of this approach in addressing the problem of system failure during data modification. | **4** | **3** | **2** | **2, 3, 9, 10** | **5** |
| **4C** | Use Autokey system, generate the ciphertext when the plaintext is "MAHETHEDEEMEDUNIVERSITY", and the key is "MITMANIPAL." | **2** | **1** | **1** | **1** | **3** |
| **5A** | Evaluate the effectiveness of the described virus structure in evading detection by exploiting file length comparison as a detection method. Consider the steps taken by the virus to compress and prepend itself to executable files and analyze how this process impacts the ability to detect the presence of the virus.<br>program CV :=<br>{goto main;<br>01234567;<br>subroutine infect-executable :=<br>{loop:<br>file := get-random-executable-file;<br>if (first-line-of-file = 01234567) then goto loop;<br>(1) compress file;<br>(2) prepend CV to file;<br>}<br>main: main-program :=<br>{if ask-permission then infect-executable;<br>(3) uncompress rest-of-file;<br>(4) run uncompressed file;}<br>} | **4** | **2** | **2** | **2** | **5** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **5B** | Utilizing the concept of inference in general-purpose databases, demonstrate how sensitive information can be derived from nonsensitive data by applying each of the three types of inference: Inference via queries based on sensitive data, Inference via DB constraints, and Inference via updates. | **4** | **3** | **2** | **2** | **3** |
| **5C** | Create a message authentication system that employs a secure hash algorithm (SHA-1) and a shared secret value (S) between the sender and receiver, ensuring authentication without offering confidentiality. | **2** | **5** | **3** | **5** | **6** |