A–1276

Total Pages : 4 **Roll No. .....**

MIT (CS)-102/CEGCS-02

(MCA/MSCCS/CEGCS)

Cyber Security Techniques

Examination February, 2026

Time : 2:00 Hrs. Max. Marks : 70

Note* :–** This paper is of Seventy (70) marks divided into Two (02) Sections 'A' and 'B'. Attempt the questions contained in these Sections according to the detailed instructions given therein. ***Candidates should limit their answers to the questions on the given answer sheet. No additional (B) answer sheet will be issued.

Section–A

(Long Answer Type Questions) (2×19=38)

***Note* :–** Section 'A' contains Five (05) Long-answer type questions of Nineteen (19) marks each. Learners are required to answer any *two* (02) questions only.

1. Explain Pretty Good Privacy (PGP) and Multipurpose Internet Mail Extensions (MIME) in detail. Discuss their history, features, working mechanisms, algorithms used, and their roles in securing email messages with examples.

2. Compare and contrast Insider Attacks and Outsider Attacks with detailed examples. Discuss differences in motive, techniques, risk level, access privileges, organizational damage, and challenges in detection and prevention.

3. Describe the Social Engineering Attack Cycle in depth. Explain each stage-research, hook, manipulation, execution, and exit strategy with detailed scenarios showing how attackers plan and carry out attacks.

4. What is a Disk Image ? Compare and contrast different imaging techniques-bit-stream image, logical image, live image, and targeted image. Discuss advantages, limitations, and use-cases for each.

5. Explain the evolution of Cyber Security Initiatives in India. Discuss major milestones, institutional developments, policy frameworks, and the changing nature of cyber threats that shaped India's cybersecurity landscape.

Section–B

(Short Answer Type Questions) (4×8=32)

***Note* :–** Section 'B' contains Eight (08) Short-answer type questions of Eight (08) marks each. Learners are required to answer any *four* (04) questions only.

1. Evaluate the statement "Firewalls cannot stop all cyber-attacks." Support your answer with examples and reasoning.

2. What is Hardware Security Module (HSM) ? Discuss its key components and functionality.

3. Evaluate the effectiveness of antivirus software in detecting modern threats like ransomware, rootkits, and zero-day exploits.

4. Explain Uniform Resource Identifiers (URI), and discuss how improper handling of URIs can lead to web-based attacks.

5. Compare and contrast Vishing, Phishing, and Smishing, on their attack mechanisms and psychological triggers.

6. Evaluate the effectiveness of the NIST Cybersecurity Framework in improving national and organizational cyber resilience, using real-world scenarios.

7. Compare and analyze the cybersecurity strategies of the United States, Canada, and India. Identify similarities and differences in their focus areas.

8. Write short notes on the following :

   (a) Deepfake-Based Scams & Identity Fraud

   (b) Dark Web

   (c) e-commerce

   (d) Cert-in

****