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

MIT (CS)-103/CEGCS-03

(MSCCS/CEGCS)

Cyber Attacks and Counter Measure : User Perspective

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. (a) Explain different types of Cyber Attacks in detail. (14)

(b) Explain difference between ALO, ARO and SLE. (5)

2. (a) Define public key cryptography in detail and explain various public key cryptography examples. (8)

(b) What is major difference between COSO and COBIT ? (6)

(c) What is information security governance ? (5)

3. (a) How compromise of information asset impact the organization ? (5)

(b) What are security controls ? What are the basic criteria based on which security controls are classified ? (4)

(c) Define SDLC. Explain different stages of SDLC with the help of a diagram. (10)

4. (a) What is Authentication ? How is it different from electronic authentication ? (4)

(b) What are the few bad password combinations that people often use in daily life ? (5)

(c) What is wireless router ? How to create wireless network ? Write steps for that. (10)

5. (a) What are the three broad categories into which the forensic tools are categorized into ? (5)

(b) What are the two basic authentication steps of Password Authentication Protocol ? Explain. (10)

(c) What are the common threats and vulnerabilities in wireless networks ? (4)

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. What is wireless router ? How to create wireless network ?

2. What is WLAN ? What are major issues with WLAN ?

3. Define preventive, detective, and corrective controls.

4. What is SSID ? How do you disable SSID ? Write step for that.

5. What are methods to safeguard your system from malicious attacks ?

6. Explain the difference between security control design and implementation.

7. Explain the difference between technical, administrative, and physical controls.

8. What is the NIST Cybersecurity Framework (CSF) ?

****