A–816

Total Pages : 3 **Roll No. .....**

MIT (CS)-103/CEGCS-03

(MSCCS/CEGCS)

(Cyber Attacks and Counter Measure : User Perspective)

1st Semester Examination, 2024 (June)

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. What is Risk Management ? Explain the activities in risk assessment process. Explain difference between qualitative and quantitative risk assessment.

2. Elaborate the term access control ? What is include in authorization process for (File, Program, Data rights) and explain the all types of control ?

3. What is Cloud Computing ? Explain all the Services provided by Cloud Computing ? Also discuss the challenges in Cloud Computing.

4. What is Digital Forensics ? Why we need the Digital Forensics ? Explain about the tools and techniques in Digital forensics ?

5. What is Cryptography ? What are the objectives of cryptography ? What are the various types of cryptographic techniques ?

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 Threat ? What are the possible sources of threats ?
2. Explain the 5 focus areas on which IT governance focuses ?
3. What is Information security governance ? What are the desired outcome of the information security governance ?
4. What is an Intrusion Detection Systems ?
5. Discuss Kerberos in detail.
6. Discuss the steps in Forensics Investigations.
7. What is the Concept of Agility and RAD ?
8. Discuss public key cryptography. Explain various public key cryptography with examples.

****