Total Page No. : 3] **[Roll No. ....**

MIT(CS)–102/CEGCS–02

MCA/MSCCS/CEGCS IIIrd/Ist Semester Examination Dec., 2023

CYBER SECURITY TECHNIQUES

Time : 2 Hours] [**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 there in. ***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 do you mean by Cyber Crime ? Discuss the nature and types of Cyber Crimes. What are the challenges before it ?

2. What is Preety good privacy ? Explain the working of PGP in detail along with diagram.

3. Explain in detail Capability maturity model in terms of cyber security.

4. What is Computer forensics ? Explain the procedure of data collection, examination, analysis and reporting used in computer forensics.

5. Explain in detail about the vision, mission, objectives and strategies mentioned in national cyber security policy of India.

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. Define attacks. Explain different types of social engineering attacks.

2. Explain about Network intrusion detection system.

3. Define Hardware Security Module. Explain the types of HSMs.

4. Define Virus. Explain the types of Computer Viruses.

5. Explain the difference between physical social engineering and computer based social engineering.

6. Define risk management. Why risk management is important in cyber security ?

7. List the cyber security initiatives taken by the government of India in recent past.

8. Write short notes on the following :

   (a) Phishing

   (b) Firewall

   (c) HTTP

   (d) Digital evidence

****