K–980

Total Page No. : 4] **[Roll No. .....**

MIT(CS)–104/CEGCS–04

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

INFORMATION SYSTEM

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. (a) What is quantum cryptography ? Which technology is used quantum cryptography ? How does quantum cryptography work ? 12

   (b) Compare the features of SHA-1 and MDS algorithm. 7

2. (a) How Digital signature differs from authentication protocols ? 5

   (b) What is Secured Electronic Transaction (SET) Protocol? Describe how purchase request, payment authorization and payment capture are done in SET ? 14

3. (a) Explain footprintinge in detail. 7

   (b) What are the *five* stages of penetration testing ? 7

   (c) What is the Diffie-Hellman algorithm for exchanging a secret session key ? 5

4. (a) Explain how Shodan can be used for intelligence gathering. 6

   (b) What do you understand by footprinting and reconnaissance in respect of Penetration testing/ Hacking ?

   (c) What are post-exploitation activities in cybersecurity, and why are they important ?

5. (a) What are the primary methods or techniques used for network scanning ?

(b) What do we understand by active and passive attacks? What are the various techniques used for carrying out these attacks ? 8

(c) What is the difference between Rijndael and AES ? 8

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. How does port scanning help in the enumeration process?

2. Why is enumeration a more intrusive process than port scanning or footprinting ?

3. How do hackers maintain access to the systems they exploit ?

4. What is DNS cache poisoning used for ?

5. What is a common tool used in post-exploitation ?

6. Explain three-way handshake using a diagram.

7. What are Honeypots ?

8. What are the risks involved in e-mail security ? How these are mitigated ?

****