

**A-817**

Total Pages : 4

Roll No. ....

**MIT (CS)-104/CEGCS-04**

**(MCA/MSCCS/CEGCS)**

**(Information System)**

3rd/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. (a) What is TCP/IP model ? What are the different functions of each of the layer in TCP IP model ? What are the protocols associated with each layer ? 10
- (b) How does email work ? 9
2. (a) Explain Data Encryption Standard (DES) in detail. How AES is used for encryption/decryption ? Discuss with example. 16
- (b) What is digital signature ? How it is useful in e-Commerce ? 3
3. (a) How does PGP create secure network ? 8
- (b) How S/MIME is better than MIME ? 6
- (c) What is a meet-in-the-middle attack ? 5
4. (a) What are the three 3 types of penetration test ? 6
- (b) What role does passive information gathering play in the footprinting process ? 7
- (c) We say that SSL/TLS is not really a single protocol, but a stack of protocols. Explain. What the different protocols in the SSL/TLS stack ? 6

5. (a) What are key distribution methods in cryptography ? 8
- (b) What can a hacker gain access to through security flaws ? 8
- (c) What do you mean by Reconnaissance ? Explain. 3

### 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 the difference between enumeration and scanning ?
2. How will attacker stay in their server to maintain access ?
3. What is the most common way for attackers to gain access to a network ?
4. Which CIA triad is most important ? What is a real-world example of the CIA triad ?
5. How to bypass UAC Windows platform ?

6. What do you understand by Rainbow Tables ?
7. What are the two types of cipher that uses symmetric key algorithm for encryption ?
8. What are the techniques used by hackers for gathering information ?

\*\*\*\*\*