

16/05/2025 TE CSE-AIML SEM-VI C-SCHEME CSS QP CODE: 10085583

Time: 3 Hours

Marks: 80

Note:

1. Question 1 is compulsory.
2. Attempt any 3 questions out of the remaining questions.

Q1. Attempt any Four.

- a. Explain different types of phishing techniques 05
- b. Explain different mechanisms to achieve security. 05
- c. Differentiate MD5 and SHA-1 algorithms. 05
- d. Explain the different modes of block ciphers. 05
- e. List and explain security requirements of database. 05

Q2.

- a. Explain RSA algorithm with example. 10
- b. List the functions of the different protocols of SSL. Explain the handshake protocol. 10

Q3.

- a. List different poly-alphabetic substitution ciphers. Encrypt "The key is hidden under the door" using playfair cipher with keyword "domestic". 10
- b. Explain memory and address protection in detail. Write a note on file protection. 10

Q4.

- a. Define digital signature. Explain any digital signature algorithm in detail. 10
- b. Explain session hijacking and management 10

Q5.

- a. Give the format of X.509 digital certificate and explain the use of a digital signature in it. 10
- b. What is need of Diffie-Hellman algorithm? Explain the algorithm with example. 10

Q6. Attempt any TWO.

- a. List and explain characteristics needed in secure hash function. Compare various hash in detail. 10
- b. Explain Triple DES in detail. 10
- c. Explain Hill cipher with example. 10

\*\*\*\*\*