Roll No. | | | | | | | | | | | | **Total No. of Pages : 02**

Total No. of Questions : 07

BCA (Sem.–6)

INFORMATION SECURITY

Subject Code : UGCA-1948

M.Code : 91695

Date of Examination:15-12-2025

Time : 3 Hrs. **Max. Marks : 60**

INSTRUCTIONS TO CANDIDATES :

1. **SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.**
2. **SECTION-B contains SIX questions carrying TEN marks each and students have to attempt any FOUR questions.**

SECTION-A

1. Write briefly:

a) How does cryptography help in securing communication?

b) What is the difference between targeted and non-targeted malicious code?

c) Can virus infect hardware?

d) How do firewalls prevent unauthorized access to a network?

e) What types of sensitive data are typically stored in a database?

f) What is public-key encryption?

g) How does ethical hacking help in improving system security?

h) How does physical security contribute to protecting sensitive data and systems?

i) What are the rights of employer?

j) Define inferential control in the context of database security.

SECTION-B

2. a) Explain the different methods of defense used in computer security to protect systems and data.

   b) Describe how substitution ciphers work. Provide an example of their use in cryptography?

3. a) How do symmetric and asymmetric encryption differ in terms of key management and security?

   b) What is targeted malicious code and how is it different from general malware? Discuss examples of targeted attacks.

4. a) What are the common memory and address protection mechanisms used by operating systems to prevent unauthorized access?

   b) What is the role of a trusted operating system in ensuring the security of a computer system? Provide examples of trusted operating systems.

5. a) Discuss the challenges in designing a multilevel database. How do these databases ensure data confidentiality and security?

   b) Explain the different types of network security controlsused to prevent unauthorized access and ensure data integrity.

6. a) Explain the process of risk analysis in security management. How does it help organizations assess vulnerabilities and mitigate potential threats?

   b) Discuss the importance of physical security in protecting sensitive data and computer systems. What measures can be taken to improve physical security?

7. What lessons can be learned from the 2017 WannaCry ransomware attack regarding corporate security practices?

NOTE: Disclosure of Identity by writing Mobile No. or Marking of passing request on any paper of Answer Sheet will lead to UMC against the Student.