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

Total No. of Questions : 07

B.Sc. (IT) (Sem.–6)

INFORMATION SECURITY

Subject Code : UGCA-1948

M.Code : 91734

Date of Examination : 18-05-23

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) What is encryption and how is it used in securing data?

b) What is a firewall and how does it protect against unauthorized access?

c) What is two-factor authentication and how does it provide additional security?

d) What is a brute force attack and how can it be prevented?

e) What is a denial-of-service attack and how can it be mitigated?

f) What is a virus and how does it infect a computer?

g) What is a phishing attack and how can it be identified and prevented?

h) What is the role of security administration in an organization?

i) What is security auditing and how does it help ensure compliance with security policies?

j) What is incident response and how does it help mitigate security incidents?

SECTION-B

2. What are some of the biggest security threats facing modern computing systems and how can they is mitigated?

3. What are the key features and properties of the Advanced Encryption Standard (AES) algorithm and how do they contribute to its strength and effectiveness in securing data?

4. What are the key principles and best practices for ensuring security in program development and how can software vulnerabilities be mitigated through proper coding techniques and testing methodologies?

5. How can operating system security measures such as access control, firewalls and intrusion detection systems be integrated with database security protocols to create a comprehensive security architecture for enterprise systems?

6. What are the different types of network attacks, such as Denial-of-Service (DoS) and Man-in-the-Middle (MitM) and how can they be prevented or mitigated using various security technologies and protocols?

7. What are the roles and responsibilities of a security administrator and what skills and qualifications are required to perform the job effectively in a fast-paced and constantly evolving security landscape?