


Name:			
Enrolment No:			
UPES End Semester Examination, December 2023			
Course: Introduction to Cybersecurity Program: MCA Course Code: CSCS7006		Semester: I Time : 03 hrs. Max. Marks: 100	
Instructions:			
SECTION A (5Qx4M=20Marks)			
S. No.		Marks	CO
Q 1	What do you understand by the AAA concept in cybersecurity?	4	CO1
Q 2	Explain in brief (i) Ransomware (ii) Viruses, (iii) Worms, (iv) Trojan Horses	4	CO2
Q 3	Define server hardening and list at least five best practices for securing a server. Explain why such practices are important.	4	CO3
Q 4	Explain the digital signature process using a block diagram. How is it used when the size of the document/message is very large?	4	CO4
Q 5	Explain the difference between event logs and audit logs. Provide examples of when each type of log is typically used in security monitoring.	4	CO5
SECTION B (4Qx10M= 40 Marks)			
Q 6	Describe the components of the CIA Triad (Confidentiality, Integrity, and Availability) and how they relate to securing data in a cybersecurity context.	10	CO1
Q 7	Describe two common vulnerabilities that endpoints can face and explain how attackers might exploit them. Additionally, discuss strategies and best practices for mitigating endpoint vulnerabilities. OR What is an RSA cryptosystem? Describe the steps used for encryption and decryption in the RSA system. What makes RSA secure?	10	CO4

Q 8	How do attackers use techniques such as phishing, DDoS attacks, and social engineering to compromise information systems? Analyze the impact of these attacks on organizations.	10	CO2
Q 9	Compare and contrast the security features of the HTTP and HTTPS protocols. What additional security measures does HTTPS provide, and why is it important for secure web communication?	10	CO5
SECTION-C (2Qx20M=40 Marks)			
Q 10	Describe the IT Security Management Framework and its components. How can this framework be utilized to establish a robust and effective cybersecurity program within an organization? Describe one example.	20	CO1
Q 11	Explore the concept of network security monitoring and its significance in identifying and mitigating cyber threats. Describe the key components and strategies involved in effective network security monitoring. OR Explain the components of Public Key Infrastructure (PKI) and the processes involved in issuing and managing digital certificates. Discuss the challenges and best practices associated with PKI implementation.	20	CO3 CO4