Semester: 2
Subject Code: 05201296
Subject Name: Cyber Security & Forensics - I

Date: 20-03-2025
Time: (1hr:30min)
Total Marks: 40

Instructions:
1. Figures to the right indicate full marks.
2. Make suitable assumptions wherever necessary.

Q.1	**Answer the following.**	**[10]**
(a)	3 short questions of 1 mark each	[3]
	(i) What is the purpose of encryption in cybersecurity?	
	(ii) Define a Trojan horse.	
	(iii) What does MAC filtering help prevent in wireless networks?	
(b)	Objective type/MCQs/True-False/Fill in blanks (7 questions of 1 mark each)	[7]
	1. What does WPA stand for in wireless security?	
	2. True or False: WPA2 is more secure than WEP. *(Justify your answer)*	
	3. Which of the following is a Denial-of-Service (DoS) attack?	
	a) Packet sniffing b) SQL Injection	
	c) Network flooding d) Cross-site scripting	
	4. Fill in the blanks: The process of verifying the identity of a user, device, or system is called _____.	
	5. What is the primary function of a firewall in network security?	
	6. Which command is used to display all active network connections in Windows?	
	7. What is the main advantage of asymmetric encryption over symmetric encryption?	
Q.2	**Answer the following. (2- or 3-mark questions)**	**[10]**
(a)	Two Questions of 2 Marks	[4]
	(i) Explain the concept of the CIA Triad in cybersecurity.	(02)
	(ii) What is a buffer overflow attack, and how does it work?	(02)
(b)	Two Questions of 3 Marks	[6]
	(i) How does Address Space Layout Randomization (ASLR) help in OS security?	(03)
	(ii) Describe how a Man-in-the-Middle (MITM) attack works and how it can be prevented.	(03)
Q.3	**Attempt any TWO.**	**[10]**
	(i) Compare and contrast WPA2 and WPA3 security protocols.	(05)
	(ii) Analyze how Zero-Day exploits pose a threat to operating system security.	(05)
	(iii) Assess the security risks associated with public Wi-Fi networks and propose countermeasures.	(05)
Q.4	**Answer the following.**	**[10]**
(a)	In what scenarios can applying the elements of the CIA triad together result in conflicts?	(05)
(b)	How can social engineering attacks compromise cybersecurity? Discuss different types of social engineering techniques and ways to prevent them.	(05)
	OR	
(b)	What are password policies, and why are they important in securing user accounts? Provide examples of strong password practices.	(05)