	P.E.S. COLLEGE OF ENGINEERING **(AN AUTONOMOUS INSTITUTE)** **CHH. SAMBHAJINAGAR-431002** **Regular Summer Examination – 2026** **Course: F.Y.M.Tech. Branch : CSE(Cyber Security) Semester : II** **Subject Code & Name:MTPESCS202T&Cyber Forensics and Cyber Laws** **Max Marks: 60 Date:01/07/2026 Duration: 3 Hr.**		
	Instructions to the Students: *1. All the questions are compulsory.* *2. The level of question/expected answer as per OBE or the Course Outcome (CO) on which the question is based is mentioned in ( ) in front of the question.* *3. Use of non-programmable scientific calculators is allowed.* *4. Assume suitable data wherever necessary and mention it clearly.*		
		(Level/CO)	Marks
Q. 1	**Solve Any one of the following.**		
A)	Explain cybercrime and information security in detail	**CO1**	**12**

Answer

1. Cybercrime (4 Marks)

Cybercrime refers to illegal activities performed using computers, digital devices, or networks. In cybercrime, the computer may act as:

- A target
- A tool
- Both target and tool

Examples

- Hacking
- Identity theft
- Cyberstalking
- Online banking fraud
- Email spoofing

Features of Cybercrime

- Easy to commit
- Difficult to trace
- Global in nature
- Causes financial and data loss

2. Types of Cybercrime (4 Marks)

a) Crimes Against Individuals

- Cyberbullying
- Identity theft
- Online harassment

b) Crimes Against Property

- Data theft
- Software piracy
- Intellectual property theft

c) Crimes Against Organizations

- Website hacking
- Database attacks
- Ransomware

d) Crimes Against Government

- Cyber terrorism

	• Attacks on government websites **3. Information Security (4 Marks)** Information security refers to protecting information and systems from un-authorized access, misuse, disclosure, or destruction. **Objectives of Information Security** 1. Confidentiality 2. Integrity 3. Availability **Security Measures** • Antivirus software • Firewalls • Encryption • Authentication systems • Backup mechanisms **Importance** • Protects sensitive data • Prevents cyberattacks • Ensures business continuity		
B)	Describe different types of cybercriminals and their motives. **Answer** **Cybercriminals** Cybercriminals are individuals or groups who use computers and networks to commit illegal activities. **Types of Cybercriminals and Their Motives** **1. Hackers (2 Marks)** People who gain unauthorized access to systems. **Motives** • Curiosity • Challenge • Financial gain **2. Crackers (2 Marks)** Hackers with malicious intentions. **Motives** • Data destruction • Stealing information • Causing damage **3. Script Kiddies (2 Marks)** Unskilled attackers using ready-made hacking tools. **Motives** • Fun • Fame • Experimentation **4. Cyber Terrorists (2 Marks)** Attack systems to create fear or disrupt society. **Motives** • Political reasons • Ideological reasons • National disruption	**CO1**	**12**

	5. Corporate Spies (2 Marks) Steal confidential business information. **Motives** • Competitive advantage • Financial profit **6. Insider Threats (2 Marks)** Employees or authorized users misusing access rights. **Motives** • Revenge • Financial gain • Personal conflicts		
Q.2	**Solve Any one of the following.**		
A)	Describe authentication service security in mobile devices. # Answer ## Authentication Service Security Authentication is the process of verifying the identity of a user before granting access to mobile devices or services. ## Types of Authentication in Mobile Devices **1. Password Authentication (2 Marks)** Users enter passwords to access devices. **2. PIN Authentication (2 Marks)** Short numeric code used for security. **3. Biometric Authentication (2 Marks)** Uses fingerprints, face recognition, or iris scanning. **4. OTP Authentication (2 Marks)** One-Time Password sent through SMS or email. **5. Multi-Factor Authentication (2 Marks)** Combines two or more authentication methods. ## Importance of Authentication Security (2 Marks) • Prevents unauthorized access • Protects sensitive information • Secures financial transactions • Reduces mobile frauds	**CO2**	**12**
B)	Explain trends in mobility and their impact on cybersecurity. # Answer ## Trends in Mobility Mobility refers to the use of portable devices and wireless communication technologies. ## Major Trends in Mobility (6 Marks) 1. Smartphones and Tablets • Used for communication and banking. 2. Cloud Computing • Data can be accessed from anywhere.	**CO2**	**12**

	3. BYOD (Bring Your Own Device) • Employees use personal devices at workplaces. 4. Mobile Banking and Payments • Online transactions through apps. 5. IoT Devices • Connected smart devices and sensors. 6. Remote Working • Employees work from remote locations. **Impact on Cybersecurity (6 Marks)** **Positive Impact** • Improved productivity • Faster communication • Easy access to services **Security Challenges** • Data leakage • Malware attacks • Unsecured Wi-Fi risks • Device theft • Phishing attacks **Preventive Measures** • Strong passwords • Encryption • VPN usage • Antivirus software		
Q. 3	**Solve Any one of the following.**		
A)	Explain DoS and DDoS attacks with examples. **Answer** **1. DoS Attack (5 Marks)** A Denial of Service (DoS) attack attempts to make a computer or network unavailable by overwhelming it with excessive traffic. **Features** • Single attacking system • Exhausts system resources **Example** Sending continuous requests to crash a website server. **Effects** • Website downtime • Service interruption • Financial loss **2. DDoS Attack (5 Marks)** A Distributed Denial of Service (DDoS) attack uses multiple infected systems (botnets) to attack a target simultaneously. **Features** • Multiple attacking systems • Large-scale attack **Example** Botnet attacking an e-commerce website during sales. **Effects**	**CO3**	**12**

	• Network congestion • Complete server failure **3. Prevention Measures (2 Marks)** • Firewalls • Intrusion Detection Systems • Traffic filtering • Load balancing • Anti-DDoS services		
B)	Discuss attacks on wireless networks and security measures. **Answer** **Wireless Network Attacks** Wireless networks are vulnerable because communication occurs through radio signals. **Types of Wireless Network Attacks (8 Marks)** **1. Eavesdropping** Attackers intercept wireless communication. **2. Rogue Access Point** Fake Wi-Fi access point created by attackers. **3. Wi-Fi Password Cracking** Attackers crack weak wireless passwords. **4. Man-in-the-Middle Attack** Attacker secretly modifies communication. **5. Denial of Service Attack** Disrupts wireless services. **6. Packet Sniffing** Capturing network packets for data theft. **Security Measures (4 Marks)** • Use WPA3/WPA2 encryption • Strong passwords • Disable unused networks • VPN usage • MAC address filtering • Regular firmware updates	**CO3**	**12**
Q.4	**Solve Any one of the following.**		
A)	Define computer forensics and explain its importance. **Answer** **Computer Forensics** Computer forensics is the process of collecting, preserving, analyzing, and presenting digital evidence in a legal manner. **Steps in Computer Forensics (4 Marks)** 1. Identification of evidence 2. Collection of evidence 3. Preservation of evidence 4. Analysis and reporting	**CO4**	**12**

	Importance of Computer Forensics (8 Marks) **1. Crime Investigation** Helps identify cybercriminals. **2. Evidence Collection** Provides digital evidence for courts. **3. Data Recovery** Recovers deleted or damaged files. **4. Fraud Detection** Detects unauthorized activities. **5. Security Improvement** Helps organizations strengthen security. **6. Legal Support** Supports legal proceedings.		
B)	Explain the digital forensics life cycle in detail. **Answer** **Digital Forensics Life Cycle** Digital forensics life cycle refers to systematic stages followed during cybercrime investigations. **Stages of Digital Forensics Life Cycle** **1. Identification (2 Marks)** Identify devices and digital evidence. **2. Preservation (2 Marks)** Protect evidence from modification. **3. Collection (2 Marks)** Acquire digital evidence using forensic tools. **4. Examination (2 Marks)** Extract useful information from evidence. **5. Analysis (2 Marks)** Analyze evidence to determine facts. **6. Presentation (2 Marks)** Prepare reports and present findings in court. **Importance** • Ensures proper investigation • Maintains evidence integrity • Supports legal proceedings	**CO4**	**12**
Q. 5	**Solve Any one of the following.**		
A)	Discuss ISO information security standards and their importance. **Answer** **ISO Information Security Standards** ISO standards provide guidelines for protecting information systems and maintaining security. **Important ISO Standards (6 Marks)** **1. ISO 27001** Information Security Management System (ISMS). **2. ISO 27002** Code of practice for information security controls.	**CO5**	**12**

	3. ISO 27005 Risk management guidelines. **4. ISO 22301** Business continuity management. **Importance of ISO Standards (6 Marks)** **1. Improves Information Security** Protects confidentiality and integrity. **2. Risk Management** Identifies and reduces risks. **3. Legal Compliance** Helps organizations meet regulations. **4. Customer Trust** Builds confidence among customers. **5. Business Continuity** Ensures smooth operations during attacks. **6. Global Recognition** Internationally accepted framework.		
B)	Describe the objectives and scope of the Information Technology Act, 2000. **Answer** **Information Technology Act, 2000** The IT Act, 2000 is India's primary cyber law dealing with electronic governance and cybercrime. **Objectives of IT Act, 2000 (6 Marks)** **1. Legal Recognition of Electronic Records** Validates electronic documents. **2. Legal Recognition of Digital Signatures** Supports secure online transactions. **3. Prevention of Cybercrime** Punishes hacking and cyber offenses. **4. Promotion of E-Commerce** Supports online business transactions. **5. E-Governance Support** Facilitates digital government services. **6. Data Protection** Protects information and privacy. **Scope of IT Act, 2000 (6 Marks)** Covers: • Cybercrimes • Electronic contracts • Digital signatures • Online banking • Data security **Important Sections** • Section 43 – Data damage • Section 66 – Hacking • Section 67 – Obscene content online	**CO5**	**12**
	***** End *****		