Reg. No.																

Question Paper Code	14474

M.E. / M.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2026

Second Semester

M.E. - Computer Science and Engineering

24PCSPC202 - SECURITY PRACTICES

Regulations - 2024

Duration: 3 Hours | Max. Marks: 100

PART – A (i) (MCQ)
(16 × 1 = 16 Marks)
Answer ALL Questions

		Marks	*K – Level*	*CO*
1.	Which of the following is a symmetric key cryptographic algorithm? a) RSA b) AES c) Diffie-Hellman d) ECC	*1*	*K1*	*CO1*
2.	An Intrusion Prevention System (IPS) differs from an Intrusion Detection System (IDS) primarily because IPS can: a) Only monitor traffic passively b) Block malicious traffic in real time c) Generate alerts only after an attack completes d) Operate exclusively at the application layer	*1*	*K2*	*CO1*
3.	Which cloud computing characteristic ensures a system continues to function even when some components fail? a) Scalability b) Elasticity c) Fault Tolerance d) Portability	*1*	*K1*	*CO1*
4.	A botnet is best described as: a) A secure VPN tunnel between two networks b) A collection of compromised devices controlled by an attacker c) A firewall that filters outgoing traffic d) A protocol for encrypting wireless communication	*1*	*K1*	*CO2*
5.	Relate which protocol is primarily used to secure data transmitted over a wireless LAN (IEEE 802.11)? a) SSL/TLS b) WPA3 c) IPsec d) S/MIME	*1*	*K2*	*CO2*
6.	Optical wireless security uses which medium for secure communication? a) Radio frequency waves b) Infrared or visible light beams c) Microwave signals d) Ultrasonic waves	*1*	*K1*	*CO2*
7.	Show which standard provides a framework for an Information Security Management System (ISMS)? a) ISO 9001 b) ISO/IEC 27001 c) NIST SP 800-53 d) PCI-DSS	*1*	*K2*	*CO3*
8.	Policy-driven system management in IT security primarily aims to: a) Manually configure each device individually b) Automate enforcement of security rules across the infrastructure c) Replace firewalls with manual monitoring d) Eliminate the need for an IDS	*1*	*K3*	*CO3*

9.	In the context of Online Identity and User Management, Single Sign-On (SSO) primarily provides: a) Multiple passwords for multiple services b) One authentication credential to access multiple services c) Biometric authentication only d) Token-based hardware authentication only	*1*	*K3*	*CO3*
10.	Identify which of the following best defines Cyber Forensics? a) Developing new encryption algorithms b) Designing secure cloud architectures c) Collecting, preserving, and analyzing digital evidence for legal proceedings d) Blocking malicious network packets in real time	*1*	*K3*	*CO4*
11.	In data encryption, choose which key is used to decrypt data encrypted with a public key? a) The same public key b) A session key c) The corresponding private key d) A symmetric key	*1*	*K3*	*CO4*
12.	Password-based authenticated key establishment protocols protect against which of the following attacks? a) SQL injection b) Zero-day application vulnerabilities c) Dictionary and brute-force attacks on session keys d) Man-in-the-middle attacks on physical cables	*1*	*K1*	*CO4*
13.	Privacy Enhancing Technologies (PETs) are designed primarily to: a) Increase internet speed b) Replace firewalls in enterprise networks c) Enable unrestricted data sharing between organizations d) Minimize personal data exposure while preserving functionality	*1*	*K2*	*CO5*
14.	A Storage Area Network (SAN) is best characterized as: a) A local area network dedicated to high-speed storage access b) A wireless sensor network for IoT devices c) A protocol suite for encrypting emails d) A type of personal cloud storage	*1*	*K3*	*CO5*
15.	Select which of the following is an example of a Physical Security Essential in an organization. a) SSL certificate management b) Cloud firewall configuration c) CCTV surveillance and biometric access control d) SQL database encryption	*1*	*K3*	*CO6*
16.	Detection of conflicts in security policies in environment monitoring systems primarily involves: a) Identifying contradictory rules that may allow or deny the same action b) Replacing all policies with a single master rule c) Ignoring overlapping policy rules d) Encrypting policy files using AES-256	*1*	*K2*	*CO6*

PART – A (ii) (Short Answer Questions)
(8 × 3 = 24 Marks)

Answer ALL Questions

17.	Identify the role of cryptography in system security.	*3*	*K3*	*CO1*
18.	Build the functions of the Domain Name System.	*3*	*K3*	*CO2*
19.	Compare IPV4 and IPV6.	*3*	*K4*	*CO3*
20.	Examine the role of forensic evidence in cybercrime investigation.	*3*	*K4*	*CO4*
21.	Solve man-in-the-middle attack using suitable technique.	*3*	*K3*	*CO5*
22.	Analyze the privacy enhancing technologies used on the internet.	*3*	*K4*	*CO6*

PART - B (Descriptive Answer Questions)
(5 × 12 = 60 Marks)
Answer ALL Questions

23.	a)	Make use of data encryption standard (DES) for ciphering a text and discuss in detail with an example.	*11*	*K3*	*CO1*
		OR			
	b)	Examine the various intrusion prevention systems and fault tolerance mechanisms used in cloud computing environments.	*11*	*K3*	*CO1*
24.	a)	Build the architecture of wireless sensor network security with its applications.	*11*	*K3*	*CO2*
		OR			
	b)	Identify the components and functions of optical network security and also state how it helps to protect from attacks.	*11*	*K3*	*CO2*
25.	a)	Examine the role of information security essentials in IT organizations.	*11*	*K4*	*CO3*
		OR			
	b)	Analyze online identity and user management systems in modern enterprises.	*11*	*K4*	*CO3*
26.	a)	Inspect how network forensic tools are used to retrieve and analyze data during the investigation process.	*11*	*K4*	*CO4*
		OR			
	b)	Examine the working of various disk structure and recovery techniques and discuss with suitable examples.	*11*	*K4*	*CO4*
27.	a)	Illustrate the working of Password based authenticated Key establishment Protocols.	*11*	*K3*	*CO5*
		OR			
	b)	Apply Forensics investigations at the Preliminary stage and Explain in detail about how information is secured during transmission.	*11*	*K3*	*CO5*
28.	a)	Identify the various privacy enhancing technologies used on the internet and explain in detail.	*11*	*K3*	*CO6*
		OR			
	b)	Illustrate storage area network security devices, risk management, and physical security essentials in detail.	*11*	*K3*	*CO6*