Reg. No.															

Question Paper Code	14146

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV/DEC 2025

Sixth Semester

Electronics and Communication Engineering

20CSOE904 - NETWORK SECURITY

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	Which of the following protocols is used to secure data transmitted over the internet? (a) HTTP (b) HTTPS (c) FTP (d) SMTP	1	K1	CO1
2.	Which one of the following is ***not*** part of the CIA triad**?** (a) Confidentiality (b) Integrity (c) Availability (d) Accountability	1	K1	CO1
3.	Which of the following is a known vulnerability of WEP? (a) Use of dynamic key rotation (b) Initialization Vector (IV) reuse (c) Mandatory mutual authentication (d) Perfect forward secrecy	1	K1	CO2
4.	What does WPA stand for in wireless security? (a) Wireless Protected Access (b) Wide Protection Authentication (c) Web Protection Access (d) Wireless Protection Access	1	K1	CO2
5.	What is the main purpose of a firewall in system-level security? (a) To provide encryption for files (b) To monitor and filter incoming and outgoing network traffic (c) To store sensitive data securely (d) To manage system resources	1	K2	CO3
6.	Which of the following is a common method for securing a system against unauthorized access? (a) Installing antivirus software (b) Using a firewall (c) Encrypting hard drives (d) All of the above	1	K1	CO3
7.	Which of the following is a common security risk in mobile devices? (a) Malware and phishing attacks (b) High-speed internet access (c) Better battery life (d) Increased processing power	1	K1	CO4
8.	Which of the following is a primary concern in securing IoT devices? (a) Device performance (b) Unauthorized access to the device and data (c) Device size (d) Device color	1	K1	CO4
9.	Which email security standard uses X.509 certificates for encryption and digital signatures? (a) PGP (b) S/MIME (c) SPF (d) DMARC	1	K1	CO5
10.	Which of the following protocol is used for securely exchanging public keys for encryption in PGP (Pretty Good Privacy)? (a) SSL/TLS (b) S/MIME (c) WebRTC (d) OpenPGP	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11.	Differentiate conventional encryption and public key encryption.	2	K2	CO1
12.	Define message digest.	2	K1	CO1
13.	Interpret any two threats specific to wireless networks.	2	K2	CO2
14.	Differentiate between WPA and WPA2 security protocols.	2	K2	CO2
15.	Infer the three main components of the Kerberos architecture.	2	K2	CO3
16.	Illustrate the function of an intrusion detection system (IDS).	2	K2	CO3
17.	Why traditional security models may not work for IoT?	2	K1	CO4

18.	Illustrate the steps in a typical patch management lifecycle.	2	K2	CO4
19.	Define SSL/TLS and explain its role in securing web communication.	2	K1	CO5
20.	Summarize how cookies should be set with the “Http Only” and “Secure” flags.	2	K2	CO5
21.	Illustrate the process of securely exchanging session keys in SSL/TLS.	2	K2	CO6
22.	Summarize the vulnerability in SSL v2 that SSL v3 addresses.	2	K2	CO6

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a) (i)	Explain the type of attacks that are handled by message authentication.	6	K2	CO1
	(ii)	Outline the steps involved in Digital signature Algorithm (DSA) with example.	5	K2	CO1
		OR			
	b) (i)	Demonstrate the AES algorithm with its key steps: SubBytes, ShiftRows, MixColumns, and AddRoundKey.	5	K2	CO1
	(ii)	Illustrate wih an example how a company is designing a secure messaging app ensure all three security goals (Confidentiality, Integrity, and Availability) are met in the design.	6	K2	CO1
24.	a) (i)	Summarize any three common wireless security threats and suggest suitable countermeasures for each.	5	K2	CO2
	(ii)	Explain the architecture of WAP and how it facilitates wireless internet access.	6	K2	CO2
		OR			
	b)	Compare WTLS with standard TLS, focusing on design optimizations for mobile devices, and analyze why WTLS may fall short in delivering robust security?	11	K2	CO2
25.	a)	Explain the steps involved in Kerberos protocol for providing authentication service.	11	K2	CO3
		OR			
	b)	Explain how firewall placement and configuration affect network security.	11	K2	CO3
26.	a)	Discuss the impact of security threats on SDN data planes and control planes.	11	K2	CO4
		OR			
	b)	Discuss the concept of a "defense in depth" security framework in network security.	11	K2	CO4
27.	a)	Explain the PGP architecture, including its key-management and Web-of-Trust model.	11	K2	CO5
		OR			
	b)	Summarize SET’s security features and limitations, focusing on how it ensures confidentiality, integrity, and non-repudiation in e-commerce.	11	K2	CO5
28.	a)	Identify the concept of Public Key Infrastructure (PKI). Discuss its components, including digital certificates, certificate authorities, and how PKI ensures secure communications.	11	K3	CO6
		OR			
	b)	Select some of the vulnerabilities that SSL v3 addressed compared to SSL v2, and explain why SSL v3 is considered more secure.	11	K3	CO6