Reg. No.															

Question Paper Code	13446

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2025

Sixth Semester

Computer Science and Engineering

(Common to 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 security goal ensures that only authorized users can access information? (a) Integrity (b) Availability (c) Confidentiality (d) Authentication	1	K1	CO1
2.	Identify the block size of DES. (a) 128 bits (b) 64 bits (c) 32 bits (d) 256 bits	1	K1	CO1
3.	What is the most secure way to lock a mobile device? (a) Simple 4-digit PIN (b) Pattern lock (c) Biometric authentication (Fingerprint/Face ID) (d) No lock	1	K1	CO2
4.	WTLS is based on which security protocol? (a) IPSec (b) TLS (Transport Layer Security) (c) SSH (d) SSL (Secure Sockets Layer)	1	K1	CO2
5.	Select the correct option: In Kerberos, the trusted third-party that issues tickets is called_____. (a) Ticket Granting Server (TGS) (b) Authentication Server (AS) (c) Key Distribution Center (KDC) (d) Certificate distribution center	1	K1	CO3
6.	The main purpose of a Trusted System is _____ (a) To encrypt all user data (b) To enforce a security policy reliably (c) To speed up computer processing (d) To provide backup and recovery services	1	K1	CO3
7.	In SDN, which component is the most common target for attackers? (a) Data Plane (b) Control Plane (c) Application Plane (d) Network Interface Card	1	K1	CO4
8.	Which of the following is a risk of not patching vulnerabilities in IoT devices? (a) Faster performance (b) Reduced storage requirements (c) Unauthorized access and data breaches (d) Improved wireless connectivity	1	K1	CO4
9.	Which of the following is an example of asymmetric encryption used in email security? (a) SHA-256 (b) AES (c) RSA (d) MD5	1	K1	CO5
10.	In SSL/TLS, what is the purpose of the server's public key? (a) To encrypt the data sent by the client (b) To decrypt the data sent by the client (c) To encrypt the symmetric session key (d) To generate the digital signature	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

		Marks	K – Level	CO
11.	Define Denial-of-Service (DoS) attack.	2	K1	CO1
12.	Differentiate between stream and block ciphers.	2	K2	CO1
13.	List the role of a wireless access point (WAP) in WLAN security.	2	K1	CO2
14.	Justify how WAP uses Secure Sockets Layer (SSL) for secure communication.	2	K2	CO2

15.	Mention the purpose of a password manager in system-level security.	2	K1	CO3
16.	List out the Requirements of Kerberos.	2	K1	CO3
17.	Define the concept of "data privacy" in cloud security for mobile and IoT.	2	K1	CO4
18.	Outline one common vulnerability in mobile device security.	2	K2	CO4
19.	Mention the term "spam" in email security.	2	K1	CO5
20.	Discuss the importance of key management in PGP.	2	K2	CO5
21.	Illustrate the purpose of the SSL handshake.	2	K2	CO6
22.	Classify the types of the TLS basic protocol.	2	K2	CO6

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Illustrate the principles of substitution and transposition ciphers in detail.	11	K2	CO1
		OR			
	b)	Demonstrate the concept of the Advanced Encryption Standard (AES) with examples.	11	K2	CO1
24.	a)	Enumerate the uses and operation of wireless LAN Security with a neat sketch.	11	K2	CO2
		OR			
	b)	Elaborate on the function of WAP end-to-end security in detail with examples.	11	K2	CO2
25.	a)	Develop the idea of X.509 authentication services and intrusion detection in detail with examples.	11	K3	CO3
		OR			
	b)	Construct the principles of firewall design and viruses with a neat sketch in detail.	11	K3	CO3
26.	a)	Generalize the idea of NFV security attack surfaces and security issues in mobile systems.	11	K3	CO4
		OR			
	b)	Develop the working of cloud security and IoT security with a diagram.	11	K3	CO4
27.	a)	Explain the operational description of Pretty Good Privacy (PGP), including its encryption and decryption process, and the role of public and private keys.	11	K2	CO5
		OR			
	b)	Explain the operation of source authentication and S/MIME with a suitable example.	11	K2	CO5
28.	a)	Explain the concept of PKI as deployed by SSL and the attacks fixed in version 3.	11	K2	CO6
		OR			
	b)	Discuss the operation of Secure Electronic Transaction (SET) with examples.	11	K2	CO6