Reg. No.												

Question Paper Code	12750

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2024

Sixth Semester

Electronics and Communication Engineering

20CSOE904 – NETWORK SECURITY

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	Differentiate passive and active security attacks. List 2 examples of passive attacks and active attacks.	2	K2	CO1
2.	Given the ciphertext "TEITARHNESHH" that was encrypted using a rail fence cipher with a depth of 3, decrypt it.	2	K2	CO1
3.	Define Wireless LAN Security.	2	K1	CO2
4.	Identify purpose of the Wireless Application Protocol (WAP).	2	K2	CO2
5.	List the 3 types of Intruders.Give example for 1 type.	2	K1	CO3
6.	Difference between rule-based anomaly detection and rule-based penetration identification.	2	K2	CO3
7.	Mention the primary security threat to Software Defined Networking (SDN).	2	K1	CO4
8.	List out the needs for data protection.	2	K1	CO4
9.	Justify how Public Key Infrastructure (PKI) support SSL/TLS in web security.	2	K2	CO5
10.	Name one common type of attack on email security.	2	K2	CO5

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a) i)	Using the Hill cipher method with the key matrix below, encrypt the plaintext message "hello". Show your work and provide the encrypted result. K= |3 2| |5 7| Note: Assume the letters of the alphabet are indexed from 0 to 25, with 'A' as 0, 'B' as 1, ..., 'I' as 8, 'H' as 7, etc.	8	K3	CO1
	ii)	Differentiate block ciphers from stream ciphers.	5	K2	CO1
		OR			
	b) i)	Compare DES and AES in terms of key length, block size, and security.	5	K2	CO1

	ii)	Explain the concept of 'S-box' in DES and how it contributes to the cipher's security.	8	K2	CO1
12.	a)	Describe the concept of Wireless Transport Layer Security and its significance.	13	K2	CO2
		OR			
	b)	Examine the potential vulnerabilities in a WAP framework and discuss the measures implemented to ensure end-to-end security in wireless communications.	13	K2	CO2
13.	a)	Consider a scenario where a user accesses multiple services in a network environment protected by Kerberos. Describe the process of obtaining and using tickets in this environment, including the acquisition of the TGT and service-specific tickets. How does the system ensure that these tickets remain secure and valid for their intended duration?	13	K2	CO3
		OR			
	b)	List and briefly describe the four techniques used to avoid guessable passwords with examples.	13	K2	CO3
14.	a)	Analyze the attack surfaces specific to Network Functions Virtualization (NFV) and recommend security measures to protect against these vulnerabilities.	13	K3	CO4
		OR			
	b)	Examine the challenges of ensuring data protection in cloud environments. Describe the strategies that could be employed to mitigate these challenges, including legal and technical measures.	13	K2	CO4
15.	a)	Evaluate the risks and threats associated with email security, detailing potential attack vectors and their mitigation strategies.	13	K5	CO5
		OR			
	b) i)	Explain how PGP provide confidentiality and authentication service to E-mail.	7	K2	CO5
	ii)	Enumerate on trusted system with neat diagram.	6	K2	CO5

PART - C (1× 15 = 15 Marks)

16.	a)	Describe the operation of Secure Electronic transaction in detail.	15	K2	CO6
		OR			
	b)	Explain the SSL/TLS handshake process, including the steps for key exchange and client-server authentication.	15	K2	CO6