Reg. No.															

Question Paper Code	13780

M.E. - DEGREE EXAMINATIONS, APRIL / MAY 2025

Second Semester

M.E. - Embedded Systems Technologies

24PESEL207 - CRYPTOGRAPHY AND NETWORK SECURITY

Regulations - 2024

Duration: 3 Hours | Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	Distinguish between active attacks and passive attacks.	2	K2	CO1
2.	List the major goals of security.	2	K1	CO1
3.	Differentiate between symmetric key and asymmetric key cryptography.	2	K2	CO2
4.	List the methods to distribute public keys.	2	K1	CO2
5.	What is a hash function?	2	K1	CO3
6.	State the three classes of authentication functions.	2	K1	CO3
7.	Mention the reasons for which a certificate can be revoked in X.509.	2	K1	CO4
8.	What is S/MIME?	2	K1	CO4
9.	What is a counterfeiting attack?	2	K1	CO6
10.	List the primary security factors.	2	K1	CO6

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

			Marks	K – Level	CO
11.	a)	Explain the basic building blocks of Advanced Encryption Standard (AES) with a neat diagram.	13	K2	CO1
		OR			
	b)	Encrypt and decrypt the text “GOOD MORNING” using (i) Playfair Cipher. (ii) Vigenere Cipher.	13	K2	CO1
12.	a)	Explain the implementation of the RSA algorithm and its attacks in detail.	13	K2	CO2
		OR			
	b)	Consider a Diffie-Hellman scheme with a common prime q= 11 and a primitive root $\alpha = 2$. a. If user A has public key $Y_A = 9$, what is A's private Key X_A? b. If user B has public key $Y_B = 3$, what is B's public key X_B? c. Calculate the shared secret key K.	13	K2	CO2

13.	a)	Explain how the Secure Hash Algorithm (SHA-512) generates message digest to provide hash functionality in detail.	*13*	*K2*	*CO3*
		OR			
	b)	Explain message encryption using symmetric and public key encryption techniques in detail.	*13*	*K2*	*CO3*
14.	a)	Explain X.509 authentication service and its associated authentication procedures in detail.	*13*	*K2*	*CO4*
		OR			
	b)	Explain IP security architecture and its features in detail.	*13*	*K2*	*CO4*
15.	a)	Explain the primary types of Intrusion Detection Systems (IDS).	*13*	*K2*	*CO6*
		OR			
	b)	Explain the specifications of 802.11 and its variants.	*13*	*K2*	*CO6*

PART - C (1 × 15 = 15 Marks)

16.	a)	Present a complete picture of firewalls, their types, configuration issues, and its limitations.	*15*	*K2*	*CO5*
		OR			
	b)	Explain rule-based intrusion detection in detail.	*15*	*K2*	*CO5*