Reg. No.															

Question Paper Code	12802

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

Second Semester

M.E - Embedded Systems Technologies

20PESEL207 - CRYPTOGRAPHY AND NETWORK SECURITY

Regulations - 2020

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.	List the requirements of an authentication function.	2	K1	CO3
6.	List the uses of MAC.	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.	Define generic decryption.	2	K1	CO5
10.	Define Distributed Denial of Service (DDoS) attacks.	2	K1	CO5

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

			Marks	K – Level	CO
11.	a)	Explain the various types of cryptographic attacks and security services specified by ITU-T X.800 with relevant examples.	13	K2	CO1
		OR			
	b)	Explain the basic building blocks of Advanced Encryption Standard (AES) with a neat diagram.	13	K2	CO1
12.	a)	Explain the implementation of the RSA algorithm and its attacks in detail.	13	K2	CO2
		OR			
	b)	Explain the implementation steps in the Diffie-Hellman key exchange algorithm.	13	K2	CO2
13.	a)	Discuss HMAC and CMAC in detail.	13	K2	CO3
		OR			

	b)	Explain message encryption using symmetric and public key encryption techniques in detail.	*13*	*K2*	*CO3*
14.	a)	Discuss Kerberos in detail.	*13*	*K2*	*CO4*
		OR			
	b)	Discuss ISAKMP protocol in detail.	*13*	*K2*	*CO4*
15.	a)	Present a complete picture of firewalls, their types, configuration issues, and its limitations.	*13*	*K2*	*CO5*
		OR			
	b)	Elaborate audit record in detail.	*13*	*K2*	*CO5*

PART - C (1 × 15 = 15 Marks)

16.	a)	Explain the primary types of Intrusion Detection Systems (IDS).	*15*	*K2*	*CO6*
		OR			
	b)	Explain the specifications of 802.11 and its variants.	*15*	*K2*	*CO6*