17 JUL 2023

Reg. No.													

Question Paper Code	12016

M.E. / M.Tech. - DEGREE EXAMINATIONS, APRIL/MAY 2023

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.	What is a transposition cipher? Give examples.	*2,K1,CO1*
2.	Distinguish between active attacks and passive attacks.	*2,K1,CO1*
3.	Differentiate between symmetric key and asymmetric key cryptography.	*2,K1,CO2*
4.	What is man-in-the-middle attack?	*2,K1,CO2*
5.	State the three classes of authentication functions.	*2,K1,CO3*
6.	Mention the requirements of a hash function.	*2,K1,CO3*
7.	What are the fields in an X.509 certificate?	*2,K1,CO4*
8.	State the services of IPSec.	*2,K1,CO4*
9.	Identify the categories of viruses.	*2,K1,CO5*
10.	Define generic decryption.	*2,K1,CO5*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a)	Explain the basic building blocks of Advanced Encryption Standard (AES) with a neat diagram.	*13,K2,CO1*
		OR	
	b)	Explain the various types of security mechanisms specified by ITU-T X.800 with relevant examples.	*13,K2,CO1*
12.	a)	Elaborate on the security issues of RSA.	*13,K2,CO2*
		OR	
	b)	Explain elliptic curve cryptography in detail.	*13,K2,CO2*
13.	a)	Explain message encryption using symmetric and public key encryption techniques in detail.	*13,K2,CO3*
		OR	

b) Discuss HMAC and CMAC in detail. *13,K2,CO3*

14. a) Explain how Pretty Good Privacy (PGP) mechanism aids to provide authentication. *13,K2,CO4*

OR

b) Explain IP security architecture and its features in detail. *13,K2,CO4*

15. a) Explain Rule-Based Intrusion Detection in detail. *13,K2,CO5*

OR

b) Elaborate on password management techniques in detail. *13,K2,CO5*

PART - C (1 × 15 = 15 Marks)

16. a) Explain the specifications of 802.11 and its variants. *15,K2,CO*

OR

b) Elaborate on the primary security factors in detail. *15,K2,CO6*