09 JAN 2023

Reg. No.												

Question Paper Code	11604

M.E. - DEGREE EXAMINATIONS, NOV/DEC 2022

Third Semester

M.E. - Computer Science and Engineering (with Specialization in Networks)

20PCNEL309 - CRYPTOGRAPHY AND WIRELESS 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 attack and threats.	*2,K1,CO1*
2.	Specify the components of encryption algorithm.	*2,K1,CO1*
3.	Perform the encryption for the plaintext M=88 using RSA algorithm p=17, q=11 and the public component e=7.	*2,K3,CO2*
4.	How digital signatures differ from authentication protocols?	*2,K4,CO2*
5.	List out the services provided by PGP.	*2,K2,CO3*
6.	Differentiate TLS and SSL security.	*2,K4,CO3*
7.	Give the security issues in wireless environment.	*2,K4,CO4*
8.	Define risk mitigation.	*2,K1,CO4*
9.	List any four security issues in 2G system.	*2,K2,CO5*
10.	Explain I- mode in GSM security.	*2,K2,CO5*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a)	Explain classical encryption techniques with symmetric cipher and hill cipher model.	*13,K2,CO1*
		OR	
	b)	(i) Define steganography. Describe the various techniques used in steganography.	*7,K2,CO1*
		(ii) Describe triple DES and its applications.	*6,K2,CO1*
12.	a)	Describe RSA Algorithm and perform encryption & decryption for the following: p=7, q=11, e=7 and m=9.	*13,K3,CO2*
		OR	
	b)	Explain the digital signature standard with necessary diagrams in detail.	*13,K2,CO2*

13. a) (i) What is Kerberos? Analyze how it provides authenticated service. *7,K4,CO3*

(ii) Explain the format of the X.509 certificate. *6,K1,CO3*

OR

b) Illustrate Intrusion Detection System (IDS) in detail with suitable diagram. *13,K4,CO1*

14. a) Explain the architecture of IEEE 802.11 WLAN and elaborate the security requirements of it. *13,K2,CO4*

OR

b) Describe the user scenario architecture and protocol stack of Bluetooth technology. *13,K2,CO4*

15. a) Demonstrate the GSM architecture and its security methods in brief. *13,K2,CO5*

OR

b) (i) Discuss authentication and key agreement in 3G. *7,K2,CO5*

(ii) How will you achieve confidentiality and data integrity in 4G communication systems? *6,K2,CO5*

PART - C (1 × 15 = 15 Marks)

16. a) (i) Explain briefly Diffie-Hellman key exchange algorithm with its merits and demerits. *10,K3,CO2*

(ii) Explain public key and when it is preferred. *5,K3,CO2*

OR

b) Illustrate the functions of firewall and describe any three types of firewall with neat diagram. *15,K3,CO3*