Reg. No.												

Question Paper Code	**12265**

M.E. / M.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2023

Third Semester

M.E. - Computer Science and Engineering (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. What is meant by Denial-of-Service attack? Is it active attack or passive attack? *2,K2,CO1*
2. Differentiate the cipher properties of confusion and diffusion. *2,K2 ,CO1*
3. What are the types of attacks are addressed by message authentication? *2,K2,CO2*
4. List the requirements of digital signature. *2,K1,CO2*
5. Define SET. What are the features of SET? *2,K1,CO3*
6. What are the various types of firewall? *2,K1,CO4*
7. List out the two limitations commonly associated with security in mobile networks. *2,K2,CO4*
8. What is the primary goal of risk mitigation in the context of wireless handheld devices? *2,K1,CO5*
9. Define I-Mode, and how does it differ from traditional mobile communication systems like GSM? *2,K1,CO6*
10. Show the major technological advancement introduced in 4G communication systems. *2,K2,CO6*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11. a) (i) Draw the functionality diagram (functionality in one round) of DES with number of bits in each flow of data. *8,K2,CO1*

(ii) Describe about the different historical techniques used for Steganography. *5,K2,CO1*

OR

b) (i) Convert the plain text "MEET ME" using Hill cipher with the given key matrix *7,K2,CO1*

$$\text{key matrix}\quad \begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$$

(ii) Illustrate the rules to perform encryption using play fair cipher and encrypt the word "Semester Result" with the keyword "Examination" using playfair cipher. *6,K2,CO1*

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create

12. a) (i) In a public-key system using RSA, you intercept the cipher text C = 20 sent to a user whose public key is e = 13, n = 77. What is the Plain text M? *8,K2,CO2*

(ii) Explain the different types of attacks on RSA. *5,K2,CO2*

OR

b) Users A and B use the Diffie-Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7.

(i) If user A has private key XA=3.What is A’s public key YA? *5,K2,CO2*

(ii) If user B has private key XB=6. What is B’s public key YB? *4,K2,CO2*

(iii) What is the shared secret key? Also write the algorithm. *4,K2,CO2*

13. a) Describe the Intrusion Detection System with suitable diagram and example *13,K2,CO4*

OR

b) Explain briefly about the different types and configurations of Firewalls *13,K2,CO4*

14. a) Discuss the security requirements for Bluetooth technology and the potential threats that these requirements aim to counter. *13,K2,CO5*

OR

b) Imagine a scenario where an organization wants to enhance the security of its WLAN. Outline a step-by-step plan, including specific security measures, to address potential vulnerabilities and threats. *13,K2,CO5*

15. a) Explain how the architecture of GSM (Global System for Mobile Communications) contributes to the security of mobile communication. Highlight key elements that play a role in securing the system. *13,K2,CO6*

OR

b) (i) How does 3GPP contribute to the development and standardization of mobile communication technologies? *5,K2,CO6*

(ii) Describe the process of Authentication and Key Agreement (AKA) in 3GPP. *6,K2,CO6*

PART - C (1 × 15 = 15 Marks)

16. a) Consider a scenario where a bank is implementing either SET or SSL/TLS for securing online banking transactions. Compare and contrast the advantages and disadvantages of each approach, considering factors such as user experience, implementation complexity, and overall security. *15,K3,CO3*

OR

b) Discuss how PGP ensures the secure transmission of the encrypted email over the internet. Explain the mechanisms in place to protect the confidentiality and integrity of the email during transit. *15,K3,CO3*