Reg. No.															

Question Paper Code	13991

M.E. / M.Tech. - DEGREE EXAMINATIONS,NOV/DEC 2025

Third Semester

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

24PCNEL309 - CRYPTOGRAPHY AND WIRELESS NETWORK SECURITY

Regulations - 2024

Duration: 3 Hours Max. Marks: 100

PART-A(MCQ)(10×1=10Marks)

Answer ALL Questions

		Marks	*K–Level*	*CO*
1.	Which of the following is *not* a security service? (a) Authentication (b) Non-repudiation (c) Confidentiality (d) Fragmentation	*1*	*K1*	*CO1*
2.	The Data Encryption Standard (DES) uses a key size of: (a) 32 bits (b) 56 bits (c) 64 bits (d) 128 bits	*1*	*K1*	*CO1*
3.	The security of the RSA algorithm is based on the difficulty of: (a) Discrete logarithm (b) Integer factorization (c) Elliptic curve (d) Matrix inversion	*1*	*K1*	*CO2*
4.	Which algorithm is used for secure key exchange over an insecure channel? (a) RSA (b) AES (c) Diffie–Hellman (d) DES	*1*	*K1*	*CO2*
5.	Which protocol provides secure authentication in distributed systems? (a) PGP (b) Kerberos (c) SSL (d) SET	*1*	*K1*	*CO3*
6.	The main purpose of a firewall is to: (a) Encrypt data (b) Detect viruses (c) Control network traffic (d) Create backups	*1*	*K1*	*CO3*
7.	Which IEEE standard defines Wireless LAN security architecture? (a) 802.3 (b) 802.5 (c) 802.11 (d) 802.15	*1*	*K1*	*CO4*
8.	Bluetooth operates under which wireless personal area network (WPAN) standard? (a) IEEE 802.15.1 (b) IEEE 802.11 (c) IEEE 802.16 (d) IEEE 802.3	*1*	*K1*	*CO4*
9.	In GSM architecture, the authentication center (AUC) is responsible for: (a) Routing calls (b) Encrypting data (c) Storing subscriber information (d) Generating authentication parameters	*1*	*K1*	*CO5*
10.	Which is the major emerging wireless security standard. (a) WEP (b) PPTP (c) SSL v2 (d) WPA3	*1*	*K1*	*CO6*

PART-B(12×2=24Marks)

Answer ALL Questions

11.	Illustrate how classical encryption techniques differ from modern encryption methods.	*2*	*K2*	*CO1*
12.	Discuss the strength and weakness of the Data Encryption Standard (DES).	*2*	*K2*	*CO1*
13.	How digital signatures ensure message integrity and non-repudiation?	*2*	*K2*	*CO2*
14.	Write the differences between hash functions and message authentication codes.	*2*	*K1*	*CO2*
15.	Define the purpose of Kerberos in network authentication.	*2*	*K1*	*CO3*
16.	State how SSL/TLS protocols provide secure communication over the Internet.	*2*	*K1*	*CO3*
17.	Develop a security model for handheld wireless devices ensuring confidentiality and integrity.	*2*	*K2*	*CO4*
18.	Demonstrate how to apply risk mitigation techniques in a wireless LAN.	*2*	*K2*	*CO4*
19.	Apply the concept of key agreement in 3GPP authentication.	*2*	*K2*	*CO5*
20.	Discuss 3G security architecture with respect to data confidentiality and integrity.	*2*	*K2*	*CO5*
21.	Build a 5 x 5 key matrix for the keyword ‘communication’ using playfair cipher method.	*2*	*K2*	*CO1*
22.	Perform encryption for the plaintext M=88 using the RSA algorithm. P=17, q=11 and public component e=7.	*2*	*K2*	*CO3*

PART-C(6×11=66Marks)

Answer ALL Questions

23. a) Encrypt the following using play fair cipher using the keyword MONARCHY. “SWARAJ IS MY BIRTH RIGHT”. Use X for blank spaces. *11 K3 CO1*

OR

b) Perform encryption and decryption using Hill cipher for the following: Message PEN and key ACTIVATED. *11 K3 CO1*

24. a) Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q=83 and a primitive root α=5. *11 K3 CO2*
(i) If Alice has a private key XA=6, what is Alice’s public key YA?
(ii) If Bob has a private key XB=10, what is Bob’s public key YB?
(iii) What is the shared secret key?

OR

b) Perform encryption and decryption using RSA algorithm for p=17, q=11, e=7 and u=88. *11 K3 CO2*

25. a) Explain the working of the Kerberos Authentication System with a neat diagram. Analyze how tickets and session keys prevent replay and impersonation attacks. *11 K2 CO3*

OR

b) Describe the different types of firewalls such as packet filtering, stateful inspection, proxy, and next-generation firewalls. *11 K2 CO3*

26. a) Analyze various attacks and security issues in mobile and wireless environments, such as eavesdropping, rogue access points, and denial-of-service (DoS). *11 K4 CO4*

OR

b) Infer how standards like WPA3, EAP, and IEEE 802.1X address security vulnerabilities and enhance overall network resilience. *11 K4 CO4*

27. a) Build a new hybrid security framework for integrating GSM and 3G systems that ensures seamless handover, authentication, and data confidentiality during inter-system communication. *11 K3 CO5*

OR

b) Model a comprehensive 3G security framework that enhances Authentication and Key Agreement (AKA) protocols by integrating mutual authentication and dynamic key generation. *11 K3 CO5*

28. a) Discuss the effectiveness of the Data Encryption Standard (DES) algorithm in securing a 64-bit plaintext using a 56-bit key. *11 K2 CO1*

OR

b) Discuss the effectiveness of the Network Security Model in protecting communication systems from modern cyber threats. *11 K2 CO1*