Reg. No.																

Question Paper Code	14623

M.E. / M.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2026

Second Semester

M.E. - Embedded Systems Technologies

24PESEL207 - CRYPTOGRAPHY AND NETWORK SECURITY

Regulations - 2024

Duration: 3 Hours | Max. Marks: 100

PART – A (i) (MCQ)
(16 × 1 = 16 Marks)
Answer ALL Questions

		Marks	K – Level	CO
1.	Which type of operation is commonly used in symmetric ciphers? a) XOR b) Division c) Modulation d) Routing	1	K1	CO1
2.	Which cipher technique uses both substitution and permutation operations? a) DES b) FTP c) SMTP d) HTTP	1	K2	CO1
3.	Which challenge must also be handled, while demonstrating the use of symmetric encryption in secure communication between two systems? a) Data compression b) Key distribution c) Error correction d) Routing	1	K3	CO1
4.	RSA consists of _____ key pair. a) Session and public b) Public and private c) Secret and session d) Dynamic and static	1	K1	CO2
5.	Which of the following is the main use of the Diffie–Hellman key exchange algorithm? a) Compression b) Key exchange c) Routing d) Authentication	1	K2	CO2
6.	Demonstration of Diffie–Hellman algorithm in establishing a secure communication system implies ____. a) Data compression b) Packet routing c) Key exchange d) Error detection	1	K3	CO2
7.	Which of the following is mainly secured using Pretty Good Privacy (PGP)? a) Databases b) E-mails c) Routers d) Wireless signals	1	K1	CO3
8.	Which encryption techniques are combined in Pretty Good Privacy (PGP)? a) Classical and modern b) Symmetric and asymmetric c) Wired and wireless d) Static and dynamic	1	K2	CO3
9.	What modification does AH protocol protects against? a) Packet b)Key c) Password d) Hardware	1	K3	CO3
10.	What is the main use of Password management? a) Routing b) Security c) Compression d) Multiplexing	1	K1	CO4

11.	What is the main purpose of designing spyware?		*1*	*K2*	*CO4*
	a) Protect	b) Steal			
	c) Compress	d) Route			
12.	Which of the following is an example of a password-cracking attack?		*1*	*K3*	*CO4*
	a) Authentication	b) Security			
	c) Intrusion	d) Compression			
13.	Application of Unauthorized access to wireless networks is called ____		*1*	*K1*	*CO5*
	a) Authentication	b) Intrusion			
	c) Compression	d) Routing			
14.	A rogue access point is a major threat to a ,		*1*	*K3*	*CO5*
	a) Wired network	b) Wireless network			
	c) Optical network	d) Satellite network			
15.	Wi-Fi Protected Access II (WPA2) improves security using,		*1*	*K2*	*CO6*
	a) Stronger encryption	b) Compression			
	c) Multiplexing	d) Routing			
16.	Eavesdropping is classified as which type of attack?		*1*	*K3*	*CO6*
	a) Passive	b) Active			
	c) Physical	d) Hardware			

PART – A (ii) (Short Answer Questions)
(6 × 3 = 18 Marks)
Answer ALL Questions

17.	Analyze the characteristics of Caesar cipher technique for encrypting a message.	*3*	*K4*	*CO1*
18.	Illustrate the role of confidentiality in symmetric encryption.	*3*	*K3*	*CO2*
19.	Compare RSA and ECC algorithms.	*3*	*K4*	*CO3*
20.	Examine the importance of key management in maintaining security protocols.	*3*	*K4*	*CO4*
21.	Apply and explain PGP mechanism used for secure e-mail transmission.	*3*	*K3*	*CO5*
22.	Illustrate the application of Wi-Fi technology in a real-time wireless communication setup.	*3*	*K3*	*CO6*

PART - B (Descriptive Answer Questions)
(6 × 11 = 66 Marks)
Answer ALL Questions

23.	a)	A plaintext "EMBEDDED SYSTEMS" is encrypted using the Vigenère cipher with the key "DATA". a) Construct the repeating key sequence. b) Encrypt the plaintext using the Vigenère table. c) Analyze how the repeating key improves security compared to the Caesar cipher.	*11*	*K4*	*CO1*
		OR			
	b)	Analyze the design criteria of DES and justify their importance in cryptographic security.	*11*	*K4*	*CO1*
24.	a)	Illustrate the implementation of the RSA algorithm by performing key generation, encryption, and decryption, and examine how common attacks can affect the RSA system.	*11*	*K3*	*CO2*
		OR			

	b)	Illustrate the working of HMAC and CMAC by demonstrating how they can be used to generate and verify a message authentication code for ensuring data integrity and authentication.	*11*	*K3*	*CO2*
25.	a)	Implement message encryption using both symmetric and public key encryption techniques to secure data transmission.	*11*	*K3*	*CO3*
		OR			
	b)	Apply DSS and RSA digital signature techniques to explain how security services such as authentication and integrity are achieved.	*11*	*K3*	*CO3*
26.	a)	Examine the X.509 authentication framework and analyze its role in Public Key Infrastructure (PKI).	*11*	*K4*	*CO4*
		OR			
	b)	Analyze various key management schemes and evaluate their effectiveness in modern network security systems.	*11*	*K4*	*CO4*
27.	a)	Apply firewall design principles to configure a secure network perimeter with an example.	*11*	*K3*	*CO5*
		OR			
	b)	Illustrate how different types of malware (virus, worm, Trojan) can affect a system and apply suitable prevention mechanisms.	*11*	*K3*	*CO5*
28.	a)	Apply security principles to analyze and mitigate common security pitfalls in a wireless network.	*11*	*K3*	*CO6*
		OR			
	b)	Elaborate on the primary security factors in detail.	*11*	*K3*	*CO6*