Reg. No.															

Question Paper Code	13487

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2025

Sixth Semester

Artificial Intelligence and Data Science

(Common to Computer Science and Engineering (AIML))

20AIEL605 - CRYPTOGRAPHY AND NETWORK SECURITY

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	Which of the following is a substitution technique? (a) Vigenère cipher (b) DES (c) RC4 (d) RSA	1	K1	CO1
2.	What is the main goal of steganography? (a) Data encryption (b) Data hiding (c) Authentication (d) Key generation	1	K1	CO1
3.	The Euclidean algorithm is used to: (a) Find inverse mod n (b) Test primarily (c) Find GCD (d) Factor numbers	1	K1	CO2
4.	What is the block size of AES? (a) 56 bits (b) 128 bits (c) 64 bits (d) 192 bits	1	K1	CO2
5.	The Chinese Remainder Theorem is useful in: (a) AES (b) Diffie-Hellman (c) ECC (d) RSA	1	K1	CO3
6.	Which algorithm uses two large prime numbers? (a) RC4 (b) DES (c) RSA (d) MD5	1	K1	CO3
7.	Which is a message authentication code? (a) MD5 (b) SHA-1 (c) HMAC (d) RSA	1	K1	CO4
8.	Kerberos is used for: (a) Encryption (b) Authentication (c) Integrity (d) Hashing	1	K1	CO4
9.	Which protocol secures email communication? (a) SSL (b) TLS (c) S/MIME (d) IPsec	1	K1	CO5
10.	Firewalls are primarily used to: (a) Encrypt data (b) Authenticate users (c) Block unauthorized access (d) Prevent phishing	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

		Marks	K – Level	CO
11.	Define perfect security.	2	K1	CO1
12.	List the different types of network security attacks.	2	K1	CO1
13.	State and explain Euler's Theorem.	2	K2	CO2
14.	What are the design principles of a block cipher?	2	K2	CO2
15.	Explain the role of key distribution in RSA.	2	K2	CO3
16.	Differentiate between symmetric and asymmetric cryptography.	2	K2	CO3
17.	Define digital signature.	2	K1	CO4
18.	What are the features of X.509 authentication service?	2	K2	CO4
19.	Write short notes on PGP.	2	K2	CO5
20.	Mention any four types of malicious software.	2	K1	CO5
21.	What is the role of an Intrusion Detection System?	2	K2	CO6
22.	Write a short note on firewall types.	2	K2	CO6

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Explain the classical encryption techniques with examples.	*11*	*K2*	*CO1*
		OR			
	b)	Explain the model for network security with neat diagram.	*11*	*K2*	*CO1*
24.	a)	Explain in detail about Groups, Rings and Fields.	*11*	*K2*	*CO2*
		OR			
	b)	Describe Modulo Arithmetic operations and properties in detail.	*11*	*K2*	*CO2*
25.	a)	Explain Chinese Remainder Theorem to solve the system: $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 2 \bmod 7$.	*11*	*K2*	*CO3*
		OR			
	b)	Describe RSA algorithm to perform encryption and decryption using RSA algorithm for the following: p=7 q=11, e=7, M=9.	*11*	*K2*	*CO3*
26.	a)	Describe in detail the key generation in AES algorithm and its expansion format.	*11*	*K2*	*CO4*
		OR			
	b)	Explain the key distribution and key management of public key encryption in detail.	*11*	*K2*	*CO4*
27.	a)	Explain briefly about the architecture and certification mechanisms in Kerberos and X.509.	*11*	*K3*	*CO5*
		OR			
	b)	Discuss about the steps involved in Signature generation and Verification functions of DSS.	*11*	*K3*	*CO5*
28.	a)	Illustrate the various types of firewalls with neat diagrams.	*11*	*K2*	*CO6*
		OR			
	b)	Describe how S/MIME is used to secure email.	*11*	*K2*	*CO6*