Reg. No.															

Question Paper Code	13567

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

Fourth Semester

Computer Science and Engineering (Cyber Security)

20SCPC401 - CRYPTOGRAPHY AND CYBERSECURITY

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	Which OSI layer is responsible for end-to-end encryption and decryption? (a) Transport (b) Network (c) Application (d) Presentation	1	K1	CO1
2.	What is the primary purpose of cryptanalysis? (a) Strengthen Security (b) Break Encryption (c) Encrypt Data (d) Generate Keys	1	K1	CO1
3.	Which block cipher encryption mode is commonly used for encrypting large amounts of data? (a) Electronic Codebook (ECB) (b) Cipher Block Chaining (CBC) (c) Output Feedback (OFB) (d) Counter (CTR)	1	K1	CO2
4.	Which of the following is NOT a block cipher? (a) Blowfish (b) RC4 (c) AES (d) DES	1	K1	CO2
5.	The Chinese Remainder Theorem is useful for which type of computations? (a) Modular arithmetic (b) Floating point operations (c) Matrix multiplication (d) Hashing	1	K2	CO3
6.	Which of the following numbers is a prime? (a) 21 (b) 51 (c) 37 (d) 63	1	K2	CO3
7.	Which of the following is a major advantage of Elliptic Curve Cryptography (ECC)? (a) It uses longer key sizes (b) It is easier to implement (c) It provides the same security as RSA with smaller key sizes (d) It does not require prime numbers	1	K2	CO4
8.	Which of the following is NOT a digital signature algorithm? (a) DSA (b) Schnorr (c) ElGamal (d) AES	1	K2	CO4
9.	Which cybercrime involves stealing sensitive information by pretending to be a trustworthy entity? (a) Phishing (b) Ransomware (c) Spoofing (d) Keylogging	1	K3	CO5
10.	Which of the following is a security risk associated with public Wi-Fi? (a) Data encryption (b) Man-in-the-Middle attacks (c) Secure VPN access (d) Firewall protection	1	K3	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11.	Define cryptography.	2	K1	CO1
12.	What is a product cryptosystem?	2	K1	CO1
13.	Differentiate between Rings and Fields.	2	K2	CO2
14.	Define avalanche effect.	2	K2	CO2
15.	Describe the chinese remainder theorem.	2	K1	CO3
16.	Define eulers totient function.	2	K1	CO3
17.	State the difference between symmetric key cryptography and public key cryptography.	2	K1	CO4
18.	What are X.509 certificates?	2	K2	CO4

19.	Define cybercrime.		*2*	*K2*	*CO5*
20.	Compare and contrast software key loggers & hardware key loggers.		*2*	*K2*	*CO5*
21.	State cross site scripting.		*2*	*K1*	*CO6*
22.	List the different types of password cracking attacks.		*2*	*K1*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a) i)	Describe various security attacks and its types.	*6*	*K2*	*CO1*
	ii)	Explain computer security concepts with diagram.	*5*	*K2*	*CO1*
		OR			
	b) i)	For the given plain text **Hello World** apply the suitable substitution technique and perform both the encryption and decryption Process.	*6*	*K2*	*CO1*
	ii)	Describe in detail about various types of Transposition Cipher Techniques.	*5*	*K2*	*CO1*
24.	a)	Explain different types of block cipher modes of operation in detail with necessary diagrams.	*11*	*K2*	*CO2*
		OR			
	b)	Discuss the key design principles of block cipher algorithms. How do these principles contribute to the security and efficiency of cryptographic systems?	*11*	*K2*	*CO2*
25.	a)	Explain briefly about Diffie-Hellman key exchange algorithm with its merits and demerits.	*11*	*K2*	*CO3*
		OR			
	b)	State Chinese Remainder Theorem and find X for the given set of congruent equations using CRT, X=1(mod5) X=2(mod7) X=3(mod9) and X=4(mod11)	*11*	*K2*	*CO3*
26.	a)	Write down the steps involved in Schnorr digital signature scheme in detail.	*11*	*K2*	*CO4*
		OR			
	b)	Describe the format of the X.509 certificate in detail.	*11*	*K2*	*CO4*
27.	a)	Explain in detail about the password cracking and types of attacks in password cracking.	*11*	*K2*	*CO5*
		OR			
	b)	Write a note on key-logger and explain in detail about types of Key-logger with necessary diagram.	*11*	*K2*	*CO5*
28.	a)	List about various tools and methods used in cyber crimes in detail.	*11*	*K2*	*CO6*
		OR			
	b)	A university faced repeated Wi-Fi security breaches due to students using unsecured devices on the network. (i) Identify the risks associated with unsecured wireless networks. (ii) Propose a wireless security framework to mitigate these risks	*11*	*K2*	*CO6*