Reg. No.																

Question Paper Code	13839

BB.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2025

Seventh Semester

Computer Science and Engineering

(Common to Information Engineering & M.Tech. - Computer Science and Engineering (5 Years Integrated))

20ITPC701 - 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 is NOT a classical encryption technique? (a) Substitution (b) Transposition (c) Steganography (d) RSA	1	K1	CO1
2.	Which of the following is an example of an active attack? (a) Eavesdropping (b) Message modification (c) Traffic analy (d) Snooping	1	K1	CO1
3.	Which of the following is a finite field used in AES? (a) GF(2) (b) GF(2^8) (c) GF(3) (d) GF(5)	1	K1	CO2
4.	Communication between end system is encrypted using a key, is known as_____ (a) Temporary key (b) Line key (c) Section key (d) Session key	1	K1	CO2
5.	In block cipher mode of operation, which mode provides both encryption and error propagation? (a) ECB (b) CBC (c) CFB (d) OFB	1	K1	CO3
6.	Which process in block ciphers involves scrambling the plaintext using secret key (a) Key generation (b) Key expansion (c) Encryption (d) Decryption	1	K1	CO3
7.	In RSA, the public key is a pair of numbers_____ (a) (p, q) (b) (n, d) (c) (n, e) (d) (e, d)	1	K1	CO4
8.	Diffie–Hellman algorithm is primarily used for: (a) Authentication (b) Key exchange (c) Digital signatures (d) Encryption only	1	K1	CO4
9.	The security of a hash function mainly depends on (a) Secrecy of the key (b) Collision resistance (c) Encryption speed (d) Data compression ratio	1	K1	CO5
10.	Firewalls can be categorized as (a) Hardware only (b) Hardware or software, or both (c) Application only (d) VPN devices only	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11.	What are security mechanisms?	2	K1	CO1
12.	How information theory related to cryptography?	2	K1	CO1
13.	Demonstrate the purpose of Euclid's algorithm in cryptography.	2	K2	CO2
14.	Outline the concept of groups and rings.	2	K2	CO2
15.	Compare AES from DES.	2	K2	CO3
16.	Classify the types of block cipher mode of operations.	2	K2	CO3
17.	How to test the given number is prime or not using Fermat's algorithm?	2	K2	CO4
18.	Explain why prime numbers are important in cryptography.	2	K2	CO4
19.	Relate how digital signature ensures the security.	2	K2	CO5

20.	Summarize three classes of MAC.		*2*	*K2*	*CO5*
21.	Outline the role of IPSec in providing secure communication over IP networks.		*2*	*K2*	*CO6*
22.	List out the security threats in wireless networks.		*2*	*K1*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Build the OSI Security Architecture and explain its components.	*11*	*K3*	*CO1*
		OR			
	b)	Encrypt the following using play fair cipher using the keyword MONARCHY. Consider plaintext as "SRISAIRAMINSTITUTIONS".	*11*	*K3*	*CO1*
24.	a)	Show Modular Exponentiation and Modulo Arithmetic operations with its properties in detail with example.	*11*	*K2*	*CO2*
		OR			
	b)	Explain Euclid's Algorithm along with two simple examples.	*11*	*K2*	*CO2*
25.	a)	Summarize the concept of AES algorithm with neat diagram.	*11*	*K2*	*CO3*
		OR			
	b)	Interpret about block cipher design principles.	*11*	*K2*	*CO3*
26.	a)	Identify the possible threats for RSA algorithm and list their counter measures. Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and M=5.	*11*	*K3*	*CO4*
		OR			
	b)	Apply Diffie-Hellman algorithm and identify the secret key shared between user A and user B using Diffie-Hellman algorithm for the following: q = 257, α (primitive root) = 3, X_A = 179 and X_B = 85. Find Public Key Y_A and Y_B.	*11*	*K3*	*CO4*
27.	a)	Rephrase the various attacks on Kerberos and write the four requirements of Kerberos.	*11*	*K2*	*CO5*
		OR			
	b)	Illustrate the SHA-1 algorithm and demonstrate how a 512-bit input message block is converted into a 160-bit message digest. Explain the steps involved in the SHA-1 process, including message padding, processing of blocks, and the final output.	*11*	*K2*	*CO5*
28.	a)	Apply the difference between PGP and S/MIME in terms of encryption methods, key management, and real-world applications.	*11*	*K3*	*CO6*
		OR			
	b)	Make use of firewall concept to explain various types of firewalls.	*11*	*K3*	*CO6*