U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

June 2025 Semester End Main Examinations

Programme: B.E. **Semester: IV**

Branch: Computer Science & Engineering **Duration: 3 hrs.**

Course Code: 23CS4ESCRP **Max Marks: 100**

Course: Cryptography

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

		UNIT - I	CO	PO	Marks
1	a)	Distinguish between active and passive attacks.	CO1	PO1	**4**
	b)	Determine if G = $<Z_{10}^{*}, X>$ is a cyclic group. Also, write all the possible cyclic subgroups.	CO1	PO1	**5**
	c)	Use Vigenere cipher with keyword "HEALTH" to decipher the following cipher text "SMFPBZIIAFMPMYL"	CO1	PO1	**5**
	d)	Analyze and find the cipher text, if the plain text "SAN" is encrypted using hill cipher with keyword as "GYBNQKURP". Also justify why a brute force attack on hill cipher is very difficult if the key is an m*m matrix.	CO2	PO2	**6**
		OR			
2	a)	A small private club has only 100 members. Calculate the number of secret keys needed for the following scenario: (Assume Symmetric key cryptography is used) i. if all members of the club need to send secret messages to each other. ii. Everyone trusts the president of the club. If a member needs to send a message to another member, she first sends it to the president; the president then sends the message to the other member. The president is also one among the 100 members.	CO1	PO1	**4**
	b)	Multiply (x^5+x^2+x) by $(x^7+x^4+x^3+x^2+x)$ in GF(2^8) using efficient multiplication algorithm. Irreducible polynomial is $(x^8+x^4+x^3+x+1)$	CO1	PO1	**5**
	c)	The encryption key in transposition cipher is (3,2,6,1,5,4) What is the decryption key?	CO1	PO1	**4**

		d)	Assuming Affine cipher is used and Eve is trying to perform chosen cipher text attack, if plain text "ab" is enciphered to "GL" i. Find both the keys k1 and k2 ii. Demonstrate how Eve carries out chosen plain text attack to decipher the following cipher text "PGDDW OYNTUTK"	*CO2*	*PO2*	**7**
			UNIT - II			
	3	a)	Imagine you are a cryptanalyst tasked with breaking a double DES encryption scheme used to secure sensitive communication between two parties. You have access to a plaintext-ciphertext pair (P,C). Devise a meet-in-the-middle attack to find the encryption keys K_1 and K_2. Justify why this attack is effective against double DES, and describe each step of the attack process in detail with neat diagram.	*CO2*	*PO2*	**5**
		b)	Design a Linear Feedback shift register with 4 cells. B4= B1 ⊕ B0. Show the key generated over 5 iterations using 1110 as seed	*CO1*	*PO1*	**5**
		c)	Justify why AES is a non-Feistel cipher. Explain any two transformations used in each round of AES.	*CO1*	*PO1*	**5**
		d)	Outline differences between modern stream cipher and block cipher.	*CO2*	*PO2*	**5**
			OR			
	4	a)	What is Confusion and Diffusion? Analyze how a product cipher achieves confusion and diffusion. With a neat diagram, illustrate the process.	*CO2*	*PO2*	**5**
		b)	Outline the key generation process of AES-128 with a neat diagram.	*CO1*	*PO1*	**5**
		c)	Demonstrate with a neat diagram key generation process in DES. Justify why '0000000 0000000' is a weak key.	*CO2*	*PO2*	**10**
			UNIT - III			
	5	a)	Outline the algorithm for square and multiply method. Apply the same to find the results for 320^{23} mod 461.	*CO1*	*PO1*	**8**
		b)	Apply Chinese remainder theorem on the following congruent equations and find the value of x $x \equiv 7 \bmod 13$ $x \equiv 11 \bmod 12$	*CO1*	*PO1*	**6**
		c)	Use Euler's theorem to find the values of the following: i) $\Phi(187)$ ii) $\Phi(35)$ iii) $60^{-1} \bmod 187$ iv) $4^{99} \bmod 35$	*CO1*	*PO1*	**6**

			OR			
	6	a)	Outline the Miller Rabin algorithm for checking primality of a given number. Apply the same to check if 109 and 271 are composite or prime. Take base=2.	*CO1*	*PO1*	**7**
		b)	Using Euler's criteria check if 16 is a quadratic residue in Z_{23}^*	*CO1*	*PO1*	**4**
		c)	Verify if $<Z^*_{38}, X>$ has primitive root? If yes, how many primitive roots are possible?	*CO1*	*PO1*	**4**
		d)	Use Fermat's theorem to compute i) $9^{794} \bmod 73$ ii) $60^{-1} \bmod 101$	*CO1*	*PO1*	**5**
			UNIT - IV			
	7	a)	Tom uses Jane's RSA public key e=7 and n=143 to send plain text P=8 encrypted as cipher text C=57. Show how can Jerry uses the chosen cipher text attack if he has access to Jane's computer to find the plain text. Assume X chosen by jerry is 2.	*CO2*	*PO2*	**6**
		b)	For a non-singular elliptic curve $y^2=x^3+ax+b$. i. Find the equation of the curve for E7(1,1) ii. Find and plot all the points on the curve	*CO1*	*PO1*	**4**
		c)	Outline key generation algorithm in ElGamal cryptosystem. In ElGamal cryptosystem, given the prime p = 31: i. If e1=13 and d=5, then calculate e2. ii. Encrypt the message "HELLO". Use 00 to 25 for encoding. Use different blocks to make P < p. iii. Decrypt the ciphertext to obtain the plaintext. Clearly show all the steps involved in encryption and decryption.	*CO2*	*PO2*	**10**
			OR			
	8	a)	Outline the RSA Asymmetric cryptography with a neat diagram. In RSA if p=3, q= 11 and e=7 and message M=5 find i) n ii) Φ (n) iii) d iv) Show how M is encrypted v) Show how cipher text is decrypted. Identify one-way function and the trapdoor in this system	*CO2*	*PO2*	**10**
		b)	Explain the process of Message Digest creation in SHA 512. Outline the structure of each round in SHA 512.	*CO1*	*PO1*	**10**
			UNIT - V			
	9	a)	Outline with a neat diagram the significance of MAC and MDC.	*CO1*	*PO1*	**6**
		b)	Assume the following values to be used in RSA Digital Signature scheme: p = 11, q = 19 and d = 23. Calculate the public key e. Then do the following:	*CO2*	*PO2*	**6**

			i. Sign and verify a message with M1 = 12 Calculate the signature S1. ii. Sign and verify a message with M2 = 25. Calculate the signature S2. iii. Show that if M = M1 × M2 = 300, then S = S1 × S2.			
		c)	Demonstrate the steps of Kerberos authentication protocol with the help of a neat diagram.	*CO1*	*PO1*	**8**
			OR			
	10	a)	With a neat diagram, explain Diffie-Hellman protocol. In the Diffie-Hellman protocol, g = 7, p = 23, Alice's private key x=3 and Bob's private key y=5. Find the value of the symmetric key. Explain the man in the middle attack with respect to Diffie-Hellman protocol.	*CO1*	*PO1*	**10**
		b)	List the three criteria to be satisfied by a cryptographic hash function.	*CO1*	*PO1*	**4**
		c)	Give the structure of X.509 Certificate format. Explain each field in detail.	*CO1*	*PO1*	**6**

****