U.S.N.										

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

Autonomous Institute Affiliated to VTU

August 2024 Supplementary Examinations

Programme: B.E. **Semester: VI**
Branch: Computer Science and Engineering **Duration: 3 hrs.**
Course Code: 20CS6PCCNS **Max Marks: 100**
Course: Cryptography and Network Security

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)	List and briefly explain the three main goals of cryptography with an example. List some passive attacks and active attacks.		CO 1	PO1	**6**
	b)	Consider a cryptosystem in which M={0,1} and Key space K={0,1,2}. Suppose the encryption matrix is as follows. Analyse this cryptosystem for perfect secrecy.		CO2	PO2	**6**
	c)	Encrypt the message "attack" using the Hill cipher with the key matrix $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$. Show the steps of encryption.		CO1	PO1	**8**
		OR				
2	a)	Use a brute-force attack to decipher the following: Assume that you know it is encrypted using an Affine cipher and that the plaintext "ab" is enciphered to "IL". The encrypted message is " eqqt aqbvuve". i. What are the possible values for the Affine cipher key parameters K_1 and K_2? ii. Decrypt the encrypted message using each possible key combination to obtain the plaintext.		CO2	PO2	**4**
	b)	Find all subgroups of the group G = $<Z_{10}^*, \times>$. Analyze whether the group is cyclic group or not? If yes, show all the generator elements.		CO2	PO2	**8**
	c)	Show how to multiply $(x^3 + x^2 + x + 1)$ by $(x^2 + 1)$ in GF(2^4) using the efficient algorithm for multiplication using irreducible polynomial:.$(x^4 + x^3 + 1)$.		CO1	PO1	**8**

KEY	Message 0	Message 1
0	0	1
1	1	0
2	0	1

			UNIT - II			
	3	a)	Create a Linear Feedback Shift Register with 4 cells in which b4 = b1 ⊕ b0. Show the value of output for 20 transitions (shifts) if the seed is $(1110)_2$.	*CO2*	*PO1*	**6**
		b)	Explain single round of DES algorithm with a neat diagram.	*CO1*	*PO1*	**6**
		c)	Write an algorithm for the AES-128 key-expansion routine.	*CO2*	*PO1*	**4**
		d)	AES has a larger block size than DES (128 versus 64). Is this an advantage or disadvantage? Justify your answer.	*CO2*	*PO2*	**4**
			UNIT - III			
	4	a)	Determine if the following integers pass the Miller-Rabin primality test or not. Use base 2: i) 109 ii) 61	*CO1*	*PO1*	**6**
		b)	State the Chinese Remainder Theorem and find X for the given set of congruent equations: X≡4 mod 5, X≡10 mod 11.	*CO1*	*PO1*	**6**
		c)	List the properties of Legendre's symbol. Solve the following Jacobi symbol: a. Jacobi(111,15) or $(\frac{111}{15})$ b. Jacobi(13,15) or $(\frac{13}{15})$	*CO1*	*PO1*	**8**
			UNIT - IV			
	5	a)	Differentiate between symmetric-key and asymmetric-key cryptosystems.	*CO2*	*PO2*	**4**
		b)	In a recent security breach, a financial institution's encrypted communication channel was compromised, leading to significant financial losses. Investigate how an attacker could have used a man-in-the-middle attack against the Diffie-Hellman key exchange to gain unauthorized access to sensitive financial information. Justify your answer with a neat diagram.	*CO2*	*PO2*	**8**
		c)	Find the private key d and perform encryption and decryption using RSA algorithm with p=3, q=11, e=7 and Message/Plaintext=5.	*CO1*	*PO1*	**8**
			OR			
	6	a)	In ElGamal, given the prime p = 31: i. Choose an appropriate e_1 and d, then calculate e_2. ii. Encrypt the following messages "H", "E" , "L"; use 00 to 25 for encoding. Use different blocks to make P<p.	*CO1*	*PO1*	**8**

		b)	Consider an elliptic curve $E_{11}(1,1)$ over a finite field 11, the generator point G is G = (6,6) . Bob choose the private value n=2. i. Find the equation of the curve. ii. Find at least five points on the curve iii. Find the public key of Bob over elliptic Curve $P_b = n\ G$.	*CO1*	*PO1*	**12**
			UNIT - V			
	7	a)	Define a cryptographic hash function. Illustrate the working of Merkle-Damgard scheme with a neat diagram.	*CO1*	*PO1*	**6**
		b)	Compare and contrast a conventional signature and a digital signature.	*CO2*	*PO2*	**6**
		c)	Using the RSA scheme, let p = 7, q = 13, and d = 29. Calculate the public key **e**. Then i. Sign and verify a message with M1 = 35. Call the signature S1. ii. Show that received message is valid with original message.	*CO2*	*PO1*	**8**

****