U.S.N.										

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

Autonomous Institute Affiliated to VTU

July 2024 Semester End Main Examinations

Programme: B.E. **Semester: V**
Branch: Computer Science and Engineering **Duration: 3 hrs.**
Course Code: 22CS5PCCRP **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.

			CO	PO	Marks
		UNIT - I			
1	a)	Use the Vigenere cipher with the keyword "HEALTH" to encrypt the message "Life is full of surprises".	CO2	PO2	**04**
	b)	Show the steps involved in multiplication of two polynomials: $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$ in $GF(2^8)$ using the efficient algorithm for multiplication using n-bit words. Consider $x^8 + x^4 + x^3 + x + 1$ as the irreducible polynomial.	CO1	PO1	**08**
	c)	Given that $Z_7 = \{1, 2, 3, 4, 5, 6\}$ * mod 7 is a group, write all the cyclic subgroups of different orders of Z_7. Is Z_7 a cyclic group?	CO1	PO1	**08**
		OR			
2	a)	Suppose we are told that plaintext "**friday**" yields the ciphertext "**pqcfku**" where Hill cipher is used (m= 2). Find the key. Show all the steps clearly.	CO2	PO2	**07**
	b)	Demonstrate with a suitable example how monoalphabetic substitution cipher is vulnerable to frequency analysis attack.	CO2	PO2	**06**
	c)	Encrypt the message "CRYPTOGRAPHY SEE" using the Affine Cipher with key (15,20). Ignore the space between words. Decrypt the message to get the plaintext.	CO2	PO2	**07**
		UNIT – II			
3	a)	Consider the linear recurrence of degree 4: $\mathbf{z_{i+4} = z_i + z_{i+1} \bmod 2}$ (a) Construct a diagram for the corresponding linear feedback shift register (LFSR). (b) Construct a table to produce the key stream generated using this LFSR with the key K= (1,0,1,1). What is its period? (c) Write down the characteristic polynomial of this linear recurrence. Is it a primitive polynomial? Explain your answer.	CO1	PO1	**06**
	b)	Let m be a message consisting of n=100 AES blocks. Alice encrypts using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number n/2 is corrupted during	CO3	PO3	**06**

			transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?			
		c)	Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES. a. XOR of subkey material with the input to the f function b. XOR of the f function output with the left half of the block c. f function d. swapping of halves of the block	CO3	PO3	**04**
		d)	Explain ShiftRows operation used in AES algorithm with an example.	CO1	PO1	**04**
			UNIT – I11			
	4	a)	Apply CRT to find an integer x which leave a remainder of 1, 2, 3, and 4 when divided by 5, 7, 9, and 11 respectively.	CO1	PO1	**06**
		b)	Find the values of the following: (a) $\phi(29)$ (b) $\phi(32)$ (c) $\phi(80)$ (d) $\phi(100)$ (e) $\phi(101)$	CO1	PO1	**05**
		c)	Apply Miller Rabin Test and check if 561 is a prime number or not.	CO1	PO1	**05**
		d)	Apply Fermat's theorem to find the values of the following: (i) $5^{15} \bmod 13$ (ii) $15^{18} \bmod 17$	CO1	PO1	**04**
			UNIT - IV			
	5	a)	For RSA with parameters: e = 7 and n = 17*31. (a) Encrypt the message block M = 2. (b) Compute a private key corresponding to the given public key. (c) Perform the decryption of the ciphertext. (d) Show if low modulus attack is possible on this message with a suitable example demonstration.	CO3	PO3	**10**
		b)	In ElGamal cryptosystem, given the prime p = 31: a. Choose an appropriate values for e_1 and d, then calculate e2. b. Encrypt the message "HELLMAN". Use 00 to 25 for encoding. Use different blocks to make P < p. c. Decrypt the ciphertext to obtain the plaintext. Clearly show all the steps involved in encryption and decryption.	CO3	PO3	**10**
			OR			
	6	a)	Consider the elliptic curve $E_{11}(2,3)$: a. Find the equation of the curve. b. Find all points on the curve and plot the points on the graph. c. Generate public and private keys for Bob. d. Choose a point on the curve as a plaintext for Alice.	CO3	PO3	**10**

			e. Create ciphertext corresponding to the plaintext in part d for Alice. f. Decrypt the ciphertext for Bob to find the plaintext sent by Alice.			
		b)	Demonstrate cycling attack on RSA cryptosystem with an example.	CO2	PO2	**05**
		c)	Explain one-way function and trapdoor one-way function with an example.	CO2	PO2	**05**
			UNIT - V			
	7	a)	Using the RSA Digital Signature scheme, let p = 809, q = 751 and d = 23. Calculate the public key e. Then do the following: a. Sign and verify a message with M1 = 101 Calculate the signature S1. b. Sign and verify a message with M2 = 51. Calculate the signature S2. c. Show that if M = M1 × M2 = 5151, then S = S1 × S2.	CO3	PO3	**10**
		b)	Explain the attacks on Digital Signature.	CO1	PO1	**05**
		c)	Analyze how digital signature satisfy the property of non-repudiation.	CO1	PO1	**05**

****