U.S.N.										

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

Autonomous Institute Affiliated to VTU

June / July 2025 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.

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)	Demonstrate different types of Cryptanalysis attacks with an example.	CO1	PO1	**05**
	b)	Use a brute-force attack to decipher the following message. Assume that you know it is an affine cipher and that the plaintext "ab" is enciphered to "GL". XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS	CO2	PO2	**05**
	c)	Encrypt the message "no matter how good you are" using the following ciphers. Ignore the space between words. Decrypt the message to get the plaintext as well. i. Affine Cipher with key (13, 7) ii. Vigenere cipher with key: "nature" iii. Autokey cipher with key = 11	CO2	PO2	**10**
		OR			
2	a)	i) Apply the extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in GF(2^5) using the irreducible polynomial $(x^5 + x^2 + 1)$. ii) Find the result of efficient algorithm used in computer implementations for multiplication using n-bit words by multiplying $(x^6 + x^4 + x + 1)$ and $(x^7 + x^6 + x^3 + x)$ in GF(2^8). Use $x^8 + x^4 + x^3 + x + 1$ as the irreducible polynomial using computer.	CO1	PO1	**10**
	b)	Let us define a new stream cipher. The cipher is affine, but the keys depend on the position of the character in the plaintext. If the plaintext character to be encrypted is in position i, we can find the keys as follow: (i) The multiplicative key is the (i mod 12)th element in Z_{26}*. (ii) The additive key is the (i mod 26)th element in Z_{26}. Encrypt the message "cryptography" using this new cipher	CO1	PO1	**05**

		c)	Use the Playfair cipher to encipher the message. The secret key can be made by filling the first and part of the second row with the word "GUIDANCE" and filling the rest of the matrix with the rest of the alphabet.	CO2	PO2	**05**
			UNIT - II			
	3	a)	Using a plaintext block of all 0s and a 56-bit key of all 0s, prove the key-complement weakness assuming that DES is made only of one round.	CO2	PO2	**05**
		b)	Write the third, fourth and fifth criteria of S-boxes and i. Use the third design criterion for S-box 3 using the following pairs of inputs. a. 000000 and 000001 b. 111111 and 111011 ii. Use the fourth design criterion for S-box 2 using the following pairs of inputs. a. 001100 and 000000 b. 110011 and 111111 iii. Use the fifth design criterion for S-box 4 using the following pairs of inputs. a. 001100 and 110000 b. 110011 and 001111	CO2	PO2	**10**
		c)	Demonstrate the creation of words for key size 128-bits in the key expansion process for AES.	CO2	PO2	**05**
			OR			
	4	a)	Consider the linear recurrence of degree 4: $z_{i+4} = z_i + z_{i+1} \bmod 2$ (i) Construct a diagram for the corresponding Linear Feedback Shift Register (LFSR). (ii) Construct a table to produce the key stream generated using this LFSR with the key K=(1,0,1,1).What is its period? (iii)Write down the characteristic polynomial of this linear recurrence. Is it a primitive polynomial? Explain your answer.	***CO3***	***PO3***	**6**
		b)	Let m be a message consisting of l=100 AES blocks. Alice encrypts using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number l/2 is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?	***CO3***	***PO3***	**6**
		c)	Compare AES and DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES. (i) XOR of subkey material with the input to the f function (ii) XOR of the f function output with the left half of the block (iii) f function (iv) Swapping of halves of the block	***CO3***	***PO1***	**8**

			UNIT - III			
	5	a)	i. Apply Miller-Rabin Test to check whether the following numbers are prime or not. Use base value as 2 for testing and then conclude on the results. (a) 271 (b) 349 Show all the steps clearly for each iteration.	CO1	PO1	**05**
		b)	i. Find the value of x for the following sets of congruence using the Chinese remainder theorem. $x \equiv 4 \bmod 5$ and $x \equiv 10 \bmod 11$ ii. Using quadratic residues, Solve $x^2 \equiv 4 \bmod 14$	CO1	PO1	**10**
		c)	Find the results of the following, using Euler's theorem: i. $12^{-1} \bmod 77$ ii. $21^{-1} \bmod 95$	CO1	PO1	**05**
			OR			
	6	a)	Apply Fermat's Little theorem to find the values of the following: (i) $5^{15} \bmod 13$ (ii) $15^{18} \bmod 17$	***CO1***	***PO1***	**5**
		b)	Find the values of the following and also write each rule: (i) $\phi(29)$ (ii) $\phi(32)$ (iii) $\phi(80)$ (iv) $\phi(100)$ (v) $\phi(101)$	***CO1***	***PO1***	**10**
		c)	Apply Miller Rabin Test and check if 561 is a prime number or not.	***CO1***	***PO1***	**5**
			UNIT - IV			
	7	a)	In ElGamal cryptosystem, given the prime p = 31: i. Choose the appropriate values for e1 and d, 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**
		b)	In the elliptic curve E(1, 2) over the GF(11) field: i. Find the equation of the curve. ii. Find at least 5 points on the curve the points on the curve and create a graph representing points on it. iii. Generate public key for Alice using private key = 3 and Generator Point (2,1). iv. Create ciphertext corresponding to the plaintext (4,2) for Alice	CO2	PO2	**10**

			OR			
	8	a)	Briefly analyse the idea behind the Elgamal cryptosystem. i) What is the one-way function in this system? ii) What is the trapdoor in this system? iii) Define the public and private keys in this system. iv) Describe the security of this system.	CO1	PO1	**06**
		b)	Illustrate any 3 attacks on the RSA cryptosystem.	CO1	PO1	**06**
		c)	Assume that Alice uses Bob's ElGamal public key (e1 = 2 and e2 = 8) to send two messages P = 17 and P′ = 37 using the same random integer r = 9. Eve intercepts the ciphertext and somehow she finds the value of P = 17. Show how Eve can use a known-plaintext attack to find the value of P′.	CO2	PO2	**08**
			UNIT - V			
	9	a)	Explain the attacks on Digital Signature	CO1	PO1	**05**
		b)	Differentiate between conventional signature and a digital signature.	CO1	PO1	**05**
		c)	Using the RSA Digital Signature scheme, let p = 11, q = 19 and d = 23. Calculate the public key e. Then do the following: a. Sign and verify a message with M1 = 12 Calculate the signature S1. b. Sign and verify a message with M2 = 25. Calculate the signature S2. c. Show that if M = M1 × M2 = 300, then S = S1 × S2.	CO1	PO1	**10**
			OR			
	10	a)	Illustrate with a neat diagram the working of Kerberos protocol. Show and justify the usage of the 3 servers-Authentication server, Ticket Granting Server and Real(data) server in Kerberos.	*CO1*	*PO1*	**10**
		b)	Draw the structure of the X.509	*CO1*	*PO1*	**2**
		c)	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?	*CO2*	*PO2*	**8**

******