U.S.N.										

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

Autonomous Institute Affiliated to VTU

February 2025 Semester End Main Examinations

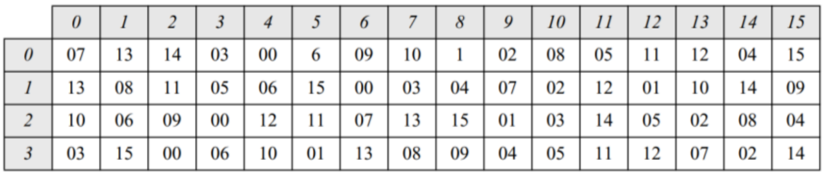
Programme: B.E. **Semester: IV**
Branch: Computer Science and Engineering **Duration: 3 hrs.**
Course Code: 23CS4ESCRP **Max Marks: 100**
Course: Cryptography

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.

			CO	PO	Marks
		UNIT - I			
1	a)	Demonstrate Playfair cipher with an example.	*CO 1*	*PO 1*	**6**
	b)	Eve has intercepted the ciphertext “UVACLYFZLJBYL”. Analyze how she can use a brute-force attack to break the Caesar cipher.	*CO 2*	*PO 2*	**6**
	c)	Multiply the following n-bit words using polynomials. (11100) × (10000) using the efficient algorithm in GF(2^5). Use ($x^5 + x^2 + 1$) as modulus.	*CO 2*	*PO 2*	**8**
		OR			
2	a)	Demonstrate Vigenere cipher with an example.	*CO 1*	*PO 1*	**6**
	b)	Alice often needs to encipher plaintext made of both letters (a to z) and digits (0 to 9). Analyse and answer the following. a. If she uses an additive cipher, what is the key domain? What is the modulus? b. If she uses a multiplication cipher, what is the key domain? What is the modulus? c. If she uses an affine cipher, what is the key domain? What is the modulus?	*CO 2*	*PO 2*	**6**
	c)	Prove that the group G = <Z_{10}*, X> is a cyclic group with two generators, g = 3 and g = 7.	*CO 2*	*PO 2*	**8**
		UNIT - II			
3	a)	Explain the Key Generation in DES with a neat figure.	*CO 1*	*PO 1*	**6**
	b)	Analyze how many of the following are there in each version of AES. a. Transformations b. Round keys c. States	*CO 2*	*PO 2*	**6**

		c)	Create a linear feedback shift register with 4 cells in which $b_4 = b_1 \oplus b0$. Show the value of output for 20 transitions (shifts) if the seed is $(0001)_2$. What is the maximum period of LFSR? Justify how to achieve this.	***CO 2***	***PO 2***	**8**
			OR			
	4	a)	Draw and explain MixColumns transformation in AES with an example	***CO 1***	***PO 1***	**6**
		b)	Write the fifth design criterion of DES and check the same for given S-box using the following pairs of inputs. a. 001100 and 110000 b. 110011 and 001111	***CO 2***	***PO 2***	**6**



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	07	13	14	03	00	6	09	10	1	02	08	05	11	12	04	15
1	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
2	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
3	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

		c)	Write the pseudocodes for SubBytes transformation and ShiftRows transformation in AES.	***CO 2***	***PO 2***	**8**
			UNIT - III			
	5	a)	Apply Fermat’s theorem to find the values of the following: (i) 5^{15} mod 13 (ii) 15^{18} mod 17	***CO 1***	***PO 1***	**6**
		b)	Find the values of the following and justify: (a) $\phi(29)$ (b) $\phi(32)$ (c) $\phi(80)$	***CO 2***	***PO 2***	**6**
		c)	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	***CO 2***	***PO 2***	**8**
			OR			
	6	a)	Solve the following using Miller-Rabin Primality test (use base 2) i. 271 ii. 349	***CO 1***	***PO 1***	**6**
		b)	Find the multiplicative inverse of the following using Euler’s theorem (i) 12^{-1} mod 77 (ii) 16^{-1} mod 323	***CO 2***	***PO 2***	**6**
		c)	Using quadratic residues, solve the following congruences: a) x2 ≡ 4 mod 7 b) x2 ≡ 5 mod 11 c) x2 ≡ 7 mod 13 d) x2 ≡ 12 mod 17	***CO 2***	***PO 2***	**8**
			UNIT – IV			
	7	a)	Demonstrate cycling attack on RSA cryptosystem with an example.	***CO 1***	***PO 1***	**6**
		b)	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′	***CO 2***	***PO 2***	**6**

		c)	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 for Alice using private key = 2 and Generator Point (1,2). iv) Create ciphertext corresponding to the plaintext (4,2) for Alice	*CO 2*	*PO 2*	**8**
			OR			
	8	a)	Draw the structure of each round in SHA- 512 and discuss on the same.	*CO 1*	*PO 1*	**6**
		b)	In an RSA system, the public key of a given user is e = 31, n=3599. Calculate the private key of this user.	*CO 2*	*PO 2*	**6**
		c)	In ElGamal cryptosystem, given the prime p = 31 a. Choose an appropriate value for e1 and d, then calculate e2. b. Encrypt the message “HELLO”. 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.	*CO 2*	*PO 2*	**8**
			UNIT - V			
	9	a)	Explain the operations involved in KERBEROS when a client process wants to access a server process.	*CO 1*	*PO 1*	**6**
		b)	In the Diffie-Hellman protocol, g = 11, p = 29, x = 5, and y = 11. Analyze and answer the following i. What is the value of the symmetric key? ii. What is the value of R1 (Alice Public Key) and R2 (Bob Public Key)? iii. Consider the above values for Alice and Bob. Demonstrate Man in the middle attack with your own value for Eve.	*CO 2*	*PO 2*	**6**
		c)	Explain the signing and verifying procedure in the RSA scheme with a neat figure. Analyse the given scenario- let p = 809, q = 751, and d = 23. Calculate the public key e. Then a. Sign and verify a message with M1 = 100. Call the signature S1. b. Sign and verify a message with M2 = 50. Call the signature S2.	*CO 2*	*PO 2*	**8**
			OR			
	10	a)	Explain RSA digital signature scheme with a neat diagram.	*CO 1*	*PO 1*	**6**
		b)	Differentiate between existential forgery and selective forgery attacks on digital signature	*CO 2*	*PO 2*	**6**
		c)	Analyze the differences in the design of Rabin scheme, Davies-Meyer scheme, Matyas-Meyer-Oseas scheme and Miyaguchi-Preneel scheme and the reason for the modifications.	*CO 2*	*PO 2*	**8**

******