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: VI**

Branch: Computer Science & 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)	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.	*CO2*	*PO2*	**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 Z26*. (ii) The additive key is the (i mod 26)th element in Z26. Encrypt the message "cryptography" using this new cipher	*CO1*	*PO1*	**5**
	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.	*CO1*	*PO1*	**5**
		OR			
2	a)	Demonstrate different types of Cryptanalysis attacks with an example.	*CO1*	*PO1*	**5**
	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	*CO1*	*PO1*	**5**
	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.	*CO1*	*PO1*	**10**

			i. Affine Cipher with key (13, 7) ii. Vigenere cipher with key: "nature" iii. Autokey cipher with key = 11			
			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*	**5**
		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	*CO1*	*PO1*	**10**
		c)	Demonstrate with a neat diagram the key generation process in DES.	*CO2*	*PO2*	**5**
			OR			
	4	a)	Demonstrate the creation of words for key size 128-bits in the key expansion process for AES.	*CO2*	*PO2*	**6**
		b)	Can you devise a meet-in-the- middle attack for a double DES? Justify your answer and show how triple DES is better than double DES.	*CO1*	*PO1*	**6**
		c)	Explain in detail about one round of DES with a neat diagram	*CO2*	*PO2*	**8**
			UNIT - III			
	5	a)	Find the value of x for the following sets of congruence using the Chinese remainder theorem. $x \equiv 4 \bmod 5$ and $x \equiv 10 \bmod 11$	*CO1*	*PO1*	**5**
		b)	Find the values of the following: i $\phi(32)$ ii $\phi(101)$ Find the results of the following, using Euler's theorem: i $12^{-1} \bmod 77$ ii $21^{-1} \bmod 95$	*CO1*	*PO1*	**10**
		c)	Using quadratic residues, Solve $x^2 \equiv 36 \bmod 143$	*CO1*	*PO1*	**5**
			OR			
	6	a)	Apply Miller-Rabin Test to check whether the following	*CO1*	*PO1*	**10**

			numbers are prime or not. Use base value as 2 for testing and then conclude on the results. (i) 109 (ii) 271 Show all the steps clearly for each iteration.			
		b)	Apply Fermat's little theorem to find the multiplicative inverse of the following: i a) 15−1 mod 17 ii b) 27−1 mod 41 Using quadratic residues, solve the following congruence: i a) $x^2 \equiv 7 \bmod 33$ ii b) $x^2 \equiv 12 \bmod 34$	*CO1*	*PO1*	**10**
			UNIT - IV			
	7	a)	Alice uses Bob's RSA public key (e = 3, n = 35) and sends the ciphertext 22 to Bob. Show how Eve can find the plaintext using the cycling attack.	*CO1*	*PO1*	**5**
		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′.	*CO2*	*PO2*	**5**
		c)	In ElGamal, given the prime p = 29, e1=3 and d=5. a. Calculate e2. b. Encrypt the message "BMSCE"; use 00 to 25 for encoding. Use different blocks to make P < p. c. Decrypt the ciphertext to obtain the plaintext.	*CO1*	*PO1*	**10**
			OR			
	8	a)	In the elliptic curve E(1,3) over the GF(13) field: a) Find the equation of the curve. b) Find all the points on the curve the points on the curve and create a graph representing points on it.	*CO1*	*PO1*	**10**
		b)	For RSA with parameters: e = 7 and p = 19, q=17. a) Write the RSA Algorithm b) Encrypt the message block M = 11. c) Compute a private key corresponding to the given public key. d) Perform the decryption of the ciphertext. e) Show if low modulus attack is possible on this message with a suitable example demonstration.	*CO1*	*PO1*	**10**
			UNIT - V			
	9	a)	Using the RSA Digital Signature scheme, let p = 11, q = 19 and	*CO1*	*PO1*	**10**

			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.			
		b)	Explain the attacks on Digital Signature	*CO1*	*PO1*	**5**
		c)	Differentiate between conventional signature and a digital signature	*CO2*	*PO2*	**5**
			OR			
	10	a)	In the Diffie-Hellman protocol, what happens if x and y have the same value, that is, Alice and Bob have accidentally chosen the same number? Are R1 and R2 the same? Do the session keys calculated by Alice and Bob have the same value? Use an example to prove your claims.	*CO2*	*PO2*	**5**
		b)	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 a real (data) server in Kerberos.	*CO1*	*PO1*	**10**
		c)	As a security analyst, you are tasked with evaluating the design of the "SecureHash" cryptographic hash function. In your analysis, you come across the Merkle-Damgard scheme, which is used as the underlying construction for this hash function. Considering the importance of the Merkle-Damgard scheme, explain its idea with neat diagram and why it plays a crucial role in the design of a cryptographic hash function like "SecureHash."	*CO2*	*PO2*	**5**

****