U.S.N.										

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

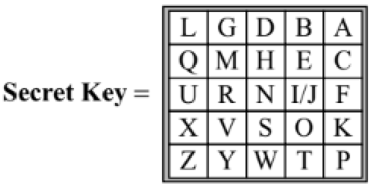
Autonomous Institute Affiliated to VTU

January / February 2025 Semester End Main Examinations

Programme: B.E. **Semester: VI**
Branch: Computer Science and Engineering **Duration: 3 hrs.**
Course Code: 22CS5PCCRP / 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)	Justify the type of security attack in each of the following cases: i. A student breaks into a professor’s office to obtain a copy of the next day’s test. ii. A student gives a check for $10 to buy a used book. Later she finds that the check was cashed for $100.	*CO1*	*PO1*	**4**
	b)	Encrypt the message “the house is being sold tonight” using the following ciphers. Ignore the space between words. Decrypt the message to get the plaintext: i. Vigenere cipher with key: “dollars”. ii. Autokey cipher with key = 7. iii. Playfair cipher with key as shown below: Secret Key = L G D B A Q M H E C U R N I/J F X V S O K Z Y W T P	*CO 3*	*PO3*	**10**
	c)	Use a Hill cipher to encipher the message “We live in an insecure world”. Use the following key: $K=\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$	*CO1*	*PO3*	**6**
		OR			
2	a)	Find the multiplicative inverse of each of the following integers in Z_{180} using the extended Euclidean algorithm. i. 132 ii. 24	*CO1*	*PO1*	**6**

		b)	Consider the plaintext = "Cryptography and Network Security" (ignore spaces) and the encryption key (3, 2, 6, 1, 5, 4). Find the decryption key and the cipher text.	*CO3*	*PO3*	**8**
		c)	Apply the extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in $GF(2^5)$ using the irreducible polynomial: $(x^5 + x^2 + 1)$	*CO1*	*PO1*	**6**
			UNIT - II			
	3	a)	AES defines three different cipher-key sizes (128, 192, and 256). DES defines only one cipher-key size (56). Discuss the advantages and disadvantages of AES over DES with respect to this difference.	*CO2*	*PO2*	**6**
		b)	Demonstrate with a neat diagram the key generation process in DES.	*CO1*	*PO1*	**6**
		c)	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*	**8**
			OR			
	4	a)	Consider the linear recurrence of degree 4: $\mathbf{z_{i+4} = z_i + z_{i+1} \bmod 2}$ (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)	Apply Miller-Rabin test to check whether the following numbers are prime or not. Use base value as 2 for testing and then	*CO1*	*PO1*	**8**

		conclude on the results: i. 109 ii. 271 Show all the steps clearly for each iteration.			
	b)	Find the value of x for the following sets of congruence using the Chinese Remainder theorem: i) $x \equiv 4 \bmod 5$, and $x \equiv 10 \bmod 11$ ii) $x \equiv 7 \bmod 13$, and $x \equiv 11 \bmod 12$	CO1	PO1	**8**
	c)	Apply Fermat's Little theorem to find the value for the following: 15^{-1} mod 17	CO1	PO1	**4**
		OR			
6	a)	Apply Fermat's Little theorem to find the values of the following: (i) 5^{15} mod 13 (ii) 15^{18} mod 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 RSA, given p=19, q=23 and e=3, find n, $\phi(n)$ and private key d.	CO3	PO3	**4**
	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	**7**
	c)	In ElGamal cryptosystem, given the prime p = 31: i. If e_1=13 and d=5, 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.	CO3	PO3	**9**

			OR			
	8	a)	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 and create a graph representing points on it. iii. Generate public key for Alice using private key = 2 and Generator Point (2,1). iv. Create ciphertext corresponding to the plaintext (4,2) for Alice.	*CO3*	*PO3*	**10**
		b)	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*	**5**
		c)	Demonstrate cycling attack on RSA cryptosystem with an example.	***CO2***	***PO2***	**5**
			UNIT - V			
	9	a)	Using the RSA Digital Signature scheme, let p = 11, q = 19 and d = 23. Calculate the public key e. Then do the following: i. Sign and verify a message with M1 = 12 Calculate the signature S1. ii. Sign and verify a message with M2 = 25. Calculate the signature S2. iii. Show that if M = M1 × M2 = 300, then S = S1 × S2.	*CO3*	*PO3*	**10**
		b)	Explain the attacks on Digital Signature.	*CO1*	*PO1*	**5**
		c)	Differentiate between conventional signature and a digital signature.	*CO1*	*PO1*	**5**
			OR			
	10	a)	Analyze how digital signature satisfy the property of non-repudiation.	*CO1*	*PO1*	**5**
		b)	With an example explain the structure of the X.509	*CO1*	*PO1*	**7**
		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**

******