U.S.N.										

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

Autonomous Institute Affiliated to VTU

August 2024 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)	Identify the different security goals and attacks in cryptography.	CO1	PO3	8
	b)	Explain how transposition techniques differ from substitution technique.	CO1	PO1	5
	c)	Illustrate with an example the encryption process of the Playfair cipher.	CO1	PO1	7
		OR			
2	a)	What is monoalphabetic cipher? Explain how it differs from Caesar cipher with an example.	CO1	PO1	8
	b)	Identify the properties of modular arithmetic operation and consider modulo 8 perform the arithmetic modulo 8 and multiplication modulo 8.	CO1	PO1	5
	c)	Explain the following with an example. i) Playfair cipher ii) Rail fence cipher iii) Vigenere cipher	CO1	PO1	7
		UNIT - II			
3	a)	Illustrate the encryption and decryption process for the Advanced Encryption standard (AES).	CO2	PO2	10
	b)	Explain in detail about the entities in the symmetric cipher model with their requirements for secure usage of the model.	CO1	PO1	5
	c)	Differentiate between Advance Encryption standard (AES) and Data Encryption Standard (DES).	CO2	PO2	5
		UNIT - III			
4	a)	Apply Fermat's theorem to find the values of the following: (i) 5^{15} mod 13 (ii) 15^{18} mod 17	CO1	PO1	6

		b)	State Chinese Remainder theorem and find the value of x for the given set of congruent equations using Chinese Remainder theorem. $X \equiv l(\text{mod } 5)$ $X \equiv 2(\text{mod } 7)$ $X \equiv 3(\text{mod } 9)$ $X \equiv 4(\text{mod } 11)$	***CO1***	***PO1***	**8**
		c)	Find the values of the following and justify: (a) $\phi(29)$ (b) $\phi(32)$ (c) $\phi(80)$	***CO1***	***PO1***	**6**
			UNIT - IV			
	5	a)	Analyze the Elliptic curve cryptography method to explain the generation of private and public key.	***CO2***	***PO2***	**5**
		b)	Outline the step-by-step procedure for generating a digest using SHA-512. Explain how an input message is handled, covering the padding scheme, processing of message blocks, utilization of the compression function and the finalization steps.	***CO1***	***PO1***	**8**
		c)	Identify main components of the ElGamal cryptosystem. Explain how the keys are generated in the ElGamal cryptosystem?	***CO1***	***PO1***	**7**
			OR			
	6	a)	Given prime numbers p=11, q=19 and value of d=17. Apply RSA algorithm for the cipher message =80 and find the plain text.	***CO1***	***PO1***	**5**
		b)	Why asymmetric key cryptographic is not suitable for large data? What are some commonly used asymmetric key algorithms?	***CO1***	***PO1***	**8**
		c)	Explain cryptographic hash function. List essential properties of a good cryptographic hash function.	***CO1***	***PO1***	**7**
			UNIT - V			
	7	a)	Demonstrate the Diffie Hellman key exchange methodology using following key values: p=11, g=2, X_A=9, X_B=4	***CO1***	***PO1***	**7**
		b)	Discuss the four requirements of Kerberos.	***CO1***	***PO1***	**4**
		c)	Discuss about the elements of X.509 Certificate.	***CO1***	***PO1***	**9**

****