VIT
Vellore Institute of Technology
CHENNAI

Reg. Number:	BAI1499

Continuous Assessment Test(CAT) – I - August 2024

Programme	:	B B.Tech and its specialization (core)	Semester	:	Fall 2024-2025
Course Code & Course Title	:	BCSE309L-Cryptography and Network Security	Class Number	:	CH2024250102290 CH2024250100560 CH2024250101332 CH2024250101335 CH2024250101336 CH2024250101657 CH2024250101002 CH2024250101007 CH2024250101017 CH2024250101024 CH2024250101032 CH2024250100559 CH2024250100557 CH2024250100558 CH2024250101028
Faculty	:	Dr.NITHYANANDAM P Dr.RENUKA DEVI S Dr.ANITA X Dr.SUBBULAKSHMI P Dr.N G BHUVANESWARI Dr.MARY SHAMALA L Dr.VATCHALA S Dr.SOBITHA AHILA S Dr.RAJESH R Dr.JANNATH NISHA O S Dr.TAPABRATA ROY Dr.KARTHIKA V Dr.VALARMATHI K Dr.SARAVANAN P Dr.RANJITH KUMAR M	Slot	:	B1+TB1
Duration	:	1 and 1/2 Hours	Max. Marks		50

Answer all questions

Q. No	Sub Sec.	Description	Marks
1	a	A cybersecurity firm is analyzing a new encryption algorithm based on modular arithmetic. The encryption method involves exponentiation with a secret key and a large prime number. To test the security of the algorithm, the firm assigns you the task of breaking the encryption by finding the secret key. The encryption works as follows: a message mmm is transformed into an encrypted value EEE using the formula: $E=g^k \bmod p$ Where you are given the following information: The base g=5 The prime number p=23 The encrypted value E=8 . Find the secret key k .	6
	b	What does it mean for two integers to be relatively prime, and can you provide examples to illustrate this concept? How is a primitive root defined in modular arithmetic, and give some examples of primitive roots for specific integers?	4

2		Imagine a detective investigating a historical case involving a secret code used by an ancient society to safeguard their treasures. The society left behind clues encoded in a system of remainders that must be deciphered to locate the treasure. Based on ancient records, you know the following conditions about the code 'X': • The code leaves a remainder of 7 when divided by 17. • The code leaves a remainder of 13 when divided by 19. • The code leaves a remainder of 5 when divided by 23. Determine the common code 'X' to unlock the treasure.	10
3		Assume that you are a security expert in an organization tasked with providing secure communication by implementing the AES algorithm for sharing secret information between your higher officials. Discuss the four different transformations of every round to encrypt the message using the AES algorithm with your higher authorities to ensure secure communication. Also, discuss the operations of function-g used in the key expansion process.	10
4		Using S-DES, Encrypt the string 01110010 using the key values K1= 10100100 and K2= 01000011. Show intermediate results after each function (IP, FK, SW, FK, IP^{-1}) using the encryption process. Find the ciphertext of the above plaintext. The S-box Values are as follows: IP = {2,6,3,1,4,8,5,7} IP^{-1} = {4,1,3,5,7,2,8,6} EP = {4,1,2,3,2,3,4,1} P4 = {2,4,3,1} S0 = $\begin{array}{c\|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array}$ S1 = $\begin{array}{c\|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$	10
5	a. b.	Let p = 11 and q= 13. Alice's public RSA key is (n, e) = (143,7). Alice receives the encrypted message C = 48. Decrypt this message using an efficient method. [7 Marks] Justify your decryption correctness by carrying out the encryption process with the answer you had arrived out of decryption in 5.a [3 Marks]	10