Reg. Number:	22BAI1266

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)
CHENNAI

Continuous Assessment Test (CAT) – I - JAN 2025

Programme	:	B.Tech.CSE and its Specializations	Semester	:	Winter 2024-25
Course Code & Course Title	:	BCSE309L & Cryptography and Network Security	Class Number	:	CH2024250502355 CH2024250502351 CH2024250502352 CH2024250502346 CH2024250502349 CH2024250501876 CH2024250501874 CH2024250502668
Faculty	:	Dr. Renuka Devi S Dr. Anita X Dr. Rajesh R Dr. Jannath Nisha O S Dr. Tapabatra Roy Dr. Kanthimathi S Dr. Logeshwari G Prof. Jai Vinita L	Slot	:	F1+TF1
Duration	:	90 minutes	Max. Mark		50

Answer all questions

1		Assume that you have received a highly confidential encrypted password "YCO" (where A =0, B = 1, C = 2, …) from your supervisor to access a server. Apply Hill cipher to decode the password using the following key matrix. $\begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$	10
2		A factory has three production lines, each producing a different product. Each production line completes a batch of products on a cycle of days: • Production Line A completes its batch every 5 days. • Production Line B completes its batch every 7 days. • Production Line C completes its batch every 11 days. All production lines started their work on the same day. However, due to maintenance delays, Production Line A was delayed by 2 days, Production Line B by 3 days, and Production Line C by 10 days. The factory manager needs to determine when all production lines will finish their batches on the same day after the delays **a.** Formulate the problem using modular arithmetic. **(2 Marks)** **b.** Find the smallest positive integer x such that all production lines will complete their batches on the same day x days after the delay. **(8 Marks)**	10

3		Suppose you are implementing AES algorithm as instructed by your organization. a) With a neat diagram describe the AES algorithm, clearly explaining the round functions. **(8 Marks)** b) Assume the 128-bit key(in hexadecimal) is given as [00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0a, 0b, 0c, 0d, 0e, 0f]. Calculate the first four words of the key expansion process. **(2 Marks)**	10
4	a) b)	List the key criteria for a good random number generator. **(3 Marks)** Consider a Linear Congruential Generator (LCG) with the parameters multiplier a=5, increment c=1, and modulus m=16. Using a starting value (seed) = 3, generate the numbers in the sequence. Evaluate the randomness of the generated sequence and check if it meets the criteria for a good random number generator. **(7 Marks)**	10
5		In a RSA encryption scheme, you are given the following public key components: n=143 and e=23. You intercept a ciphertext C=9. a. Calculate the plaintext M corresponding to the intercepted ciphertext C=9 using the provided key components **(7 marks).** b. To ensure the accuracy of the decryption, re-encrypt the plaintext M using public key (e, n) and confirm that it matches the original intercepted ciphertext C=9 **(3 marks).**	10

**********All the best **********