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

Reg. Number:	22BRS1243

Continuous Assessment Test (CAT) – II - MARCH 2025

Programme	:	B.Tech.CSE and its Specializations	Semester	:	Winter 2024-25
Course Code & Course Title	:	BCSE309L & Cryptography and Network Security	Class Number	:	**CH2024250502360 CH2024250502358 CH2024250502356 CH2024250501881 CH2024250501885 CH2024250502671 CH2024250502670 CH2024250502357**
Faculty	:	**Dr. ANITA X. Dr. RAJESH R. Dr. JANNATH NISHA O.S. Dr. LEKI CHOM THUNGON Dr. LOGESWARI G Dr. ROLLA SUBRAHMANYAM Prof. JAI VINITA L Dr. LINDA JOSEPH**	Slot	:	F2+TF2
Duration	:	**1 ½ Hours**	Max. Mark		50

Answer all questions

1		A tech company is developing a secure messaging platform using ElGamal encryption. Buddy, a security analyst, wants to securely receive a confidential report from Aria. To ensure security, Buddy selects a prime number 23, a generator 5, and a private key 6. He then computes his public key and shares it with Aria. Aria, preparing to send the report (represented as the number 10), selects a random integer 3 and encrypts the message. She then sends the encrypted message to Buddy, who decrypts it to retrieve the original report. a. What is Buddy's public key, and how is it generated? (2 Marks) b. How does Aria encrypt the message, and what ciphertext does she send to Buddy? (3 Marks) c. How does Buddy decrypt the message, and what steps does he follow to retrieve the original report? (3 Marks) In what ways does ElGamal encryption ensure the confidentiality of Aria's message? (2 Marks)	10
2		Two parties agree to make use of a key exchange protocol, without knowing that this protocol could pose a threat of their key being exposed. Now, the two parties agree on the prime number as 13 and 6 as primitive root of 13. They use their private keys as 5 and 4 respectively. An intruder, during a random usage of the network, finds out the public keys of the two parties and replaces them with his own public keys. He prepares for the attack by generating two random private keys as 7 and 3 respectively. Enumerate the steps taken by the intruder to get hold of the keys that are exchanged by the two parties to perform eavesdropping and modification.	10

		Compute the secret keys generated between intruder and the legitimate users.	
3		A software company uses MD5 to verify the integrity of files downloaded by users. Identify the basic arithmetic and logical functions used in MD5 and calculate MD5 single-round primitive function values for F (B, C, D) and I (B, C, D) Given, A:0x00010203 B:0x04050607 C:0x08090a0b D:0x0c0d0e0f	10
4		In a secure financial transaction system, Alex and Jordan are using elliptic curve cryptography to transmit confidential transaction data. They have agreed to use an elliptic curve defined by the parameters p = 11, a = 1, and b = 6, with the base point G = (2, 7). Alex, who is initiating the transaction, wants to securely transmit the point T = (3, 5) to Jordan. To do so, Alex selects a random integer k = 3 for the encryption process. Jordan, on the receiving end, has a private key of 2. Outline and compute the encryption process Alex would follow to securely send the transaction point (T = (3,5)) using the given elliptic curve parameters, generator, and random integer k.	10
5		A dealer D shares a secret key 25 between 5 players using a random polynomial of degree 2 by framing the equation with random values for a1 and a2. Demonstrate how many shares are required to reconstruct the secret. Show the stepwise procedure to distribute the secret and to reconstruct the secret.	10

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