150

Reg. No.: 21BCE5972

Name :

VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Continuous Assessment Test-I - February 2024

Programme	:	B.Tech.	Semester	:	Winter 2023 – 2024
Course Code & Title	:	BCSE309L-Cryptography and Network Security	Class Nbr	:	CH2023240501438 CH2023240501461 CH2023240501468 CH2023240501444 CH2023240501448 CH2023240501477 CH2023240501483 CH2023240501453 CH2023240501490 CH2023240501495 CH2023240501501 CH2023240501458
Faculty	:	Dr. ANITA X Dr. SUBBULAKSHMI P Dr. BHUVANESWARI AMMA N G Dr. MARY SHAMALA L Dr. VATCHALA S Dr. SOBITHA AHILA S Dr. RAJESH R Dr. TAPABRATA ROY Dr. KARTHIKA V Dr. BALASARASWATHI Dr. KANTHIMATHI S Dr. VALARMATHI K	Slot	:	F2+TF2
Duration	:	1 ½ Hours	Max. Marks	:	50

Answer all Questions

1. i) Imagine you're a cryptographer working with an ancient secure communication system. Your task is to find the secret value of X using the Extended Euclidean algorithm such that 79.X ≡ 1 mod 3220. (6 Marks)

   ii) Determine if the integer 2 has the special property of a primitive root about the prime number 13. If it does, proceed to create a discrete logarithm table using 2 as the base, modulo 13. (4 Marks) **10**

79 9.

2. i) In a secure communication system, a message has been encoded into multiple parts, each part being sent to a different receiver. Each receiver gets a congruence equation representing their part of the encoded message. To decode the original message, all parts of the encoded message must be combined. Decode the original message represented by the following set of congruence equations

$X \equiv 3 \pmod{7}$
$X \equiv 3 \pmod{5}$
$X \equiv 4 \pmod{12}$ (8 Marks) 10

ii) Explain why a solution might not exist for the following system of congruences:

$X \equiv 3 \pmod{6}$
$X \equiv 4 \pmod{8}$ (2 Marks)

3. i) Neha and Megha are studying third-year B.Sc., Physics. During the Quantum Physics class, Neha wants to send a message to Megha in a confidential manner so that no one notices her. The message is "TCEM". Apply the Hill cipher method for encryption using the key value $\begin{pmatrix} 17 & 8 \\ 19 & 3 \end{pmatrix}$. Extract the original message by using the same Cipher method. (6 Marks)

TMSB

10

ii) Yes Bank for its online banking wants to ensure the confidentiality and integrity of financial transactions conducted over the internet. The bank authority decides to communicate securely using AES (Advanced Encryption Standard). They choose a 128-bit key for AES encryption. Suggest an algorithm for generating subkeys. Also, determine the first four words of the key expansion process for the following key: 67 20 46 75 20 4B 75 6E 73 20 6D 79 54 68 61 74 (4 Marks)

[illegible] in [illegible]

4. Imagine you are working in a defense department and are in a position to develop a secure communication system that needs to send multiple blocks of messages. Compare and contrast the block cipher modes of operation required for secure communication with illustration. 10

Very [illegible]

5. Suppose Alice and Bob use an Elgamal scheme with a common prime q = 157 and a primitive root α = 5.

i) If Bob has public key $Y_B = 10$ and Alice chose the random integer k = 3, what is the ciphertext of M = 9? (5 Marks) 10

ii) If Alice now chooses a different value of k so that the encoding of M = 9 is C = (25, C_2), what is the integer C_2? (5 Marks)

[illegible]

C =

P =

(E,E+D)

[illegible]

G