REG.NO.:

VIT

Vellore Institute of Technology

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

School of Computer Science Engineering and Information Systems

CONTINUOUS ASSESSMENT TEST - I SLOT: C1+TC1

WINTER SEMESTER 2024-2025

Programme Name & Branch : B.Tech (IT)

Course Code and Course Name : Network and Information Security & BITE4011L

Faculty Name(s) : Dr.Shantharajah S P, Dr.Aswani Kumar Cherukuri, Dr.Mangayarkarasi R

Class Number(s) : VL2024250503088, VL2024250503076, VL2024250503083

Date of Examination : 29-01-2025

Exam Duration : 90 minutes **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- BL – Blooms Taxonomy Level (2 – Understand, 3 – Apply, 4- Analyzing)
- Course Outcomes: 1. Understand the security principles and mechanisms.
  2. Analyze and evaluate cryptographic primitives

Q.No.	Question	Max Marks	CO	BL
1.	(a) Consider an ATM machine of a bank in which users provide a personal identification number (PIN) and a card for account access. How does confidentiality, integrity, and availability are maintained for the safer transaction of this banking system. Give examples of each secure services.	5	CO1	BL2
	(b) Perform the Playfair cipher technique for the given plaintext "GREENOS" and obtain the Cipher text for the key "BOYFRIENDS".	5	CO1	BL3
2.	Compute the AES Mix column process for the given values and derive the new bytes to fill the mentioned two columns. Show the computations in detail to derive the value for the '?' column. $\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} D4 & & & \\ BF & & & \\ 5D & & & \\ 30 & & & \end{bmatrix} = \begin{bmatrix} 04 & & & \\ ? & & & \\ ? & & & \\ & & & \end{bmatrix}$	10	CO2	BL4
3.	Write about the popular symmetric algorithm that derives the concept of Feistel cipher structure and discuss one round structure of the same algorithm in detail with a neat sketch.	10	CO2	BL2
4	How does multiple encryptions of DES be effective from attacks? Describe its concepts along with the way of handling multiple keys in detail.	10	CO2	BL2
5.	(a) Compute $\phi(1000)$.	2	CO2	BL3
	(b) Solve and find the value for 29^5 **mod 100** using Modular exponential simplification method.	4	CO2	BL3
	(c) Find the Multiplicative inverse of **103 mod 676** using Extended Euclidean Algorithm.	4	CO2	BL3

****