VIT-AP UNIVERSITY	**Continuous Assessment Test - 1 | Fall Semester (2025-26) - August 202**	
	Maximum Marks: 50	Duration: 90 Minutes
Course Code: SWE3003	Course Title: Information and System Security	
Set No: 03	Exam Type : **Closed Book**	School: SCOPE
Date: 20/08/25	Slot: C1	Session: FN

Keeping mobile phone/smart watch, even in 'off' position is treated as exam malpractice

General Instructions if any

1. **"*fx* series" - non-Programmable calculator is permitted: YES**
2. **Reference tables permitted: NO**

PART – A: Answer any ALL Questions, Each Question Carries 10 Marks (5×10=50 Marks)

1. Alice and Bob are cryptographers working to secure a confidential communication system. To prevent enemy agents from intercepting and understanding their messages, they use the Hill Cipher for encryption. Alice needs to send Bob the message "CAT," where each letter is represented by its alphabetical position. Alice uses the following 3×3 matrix over mod 23 as the encryption key matrix. **(10M)**

$$\begin{bmatrix} 2 & -3 & 5 \\ -1 & 4 & -2 \\ 6 & -5 & 3 \end{bmatrix}$$

2. Use the extended Euclidean algorithm to find the inverse of $(x^3 + x^2 + 1)$ in GF (2^5) with the irreducible polynomial $(x^5 + x^2 + 1)$. **(10 M)**

3. Imagine that two diplomats, Sarah and Ahmed, are communicating via secure messages to discuss a highly sensitive peace treaty. To ensure that their messages cannot be easily intercepted and understood by unauthorized parties, they decide to use the Affine Cipher for encryption over modulus 21. Sarah wants to send Ahmed the message "PEACE". Explain the steps involved in the encryption and decryption process of the message with the keys a=11 and b =19. **(10 M)**

4. Identify and justify your answer in detail in terms of security attack or security mechanism or security service. **(10M)**
   - Emma is transmitting sensitive financial data to her company's headquarters. To prevent eavesdroppers from intercepting the data on a single communication path, her system uses **route diversity**. This technique selects and continuously changes different available network routes for transmitting packets of data.
   - a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.
   - Rachel is selling her car to James, and they agree on all the terms of the sale, including the price and transfer date. To finalize the deal, Rachel prepares a digital contract as proof of the transaction. To ensure the contract is valid and tamper-proof, Rachel and James use a trusted online platform that verifies their identities and securely records their agreement.
   - A bank customer service representative refuses to share account details over the phone unless the caller provides a preassigned security PIN that was set up during account creation.

- The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

5. Explain the following cryptographic terms in detail.
   - Relation between Services and Mechanisms (5M)
   - Notarization (2M)
   - Denial of Service (3M)

QP MAPPING

Q. No.	E/A/T	Module Number	Marks	BL	CO Mapped	PO Mapped	PEO Mapped	PSO Mapped
Q1	E	2	10	2	2	1,2	-	-
Q2	A	2	10	1	2	1,2	-	-
Q3	T	2	10	3	2	1,2	-	-
Q4	A	1	10	4	1	1	-	-
Q5	A	1	10	2	1	1	-	-