St. MARTIN'S ENGINEERING COLLEGE

UGC Autonomous
NBA & NAAC A+ Accredited
Dhulapally, Secunderabad-500 100
www.smec.ac.in

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE (AI & DS)

ASSIGNMENT-I

Course Name : CRYPTOGRAPHY AND NETWORK SECURITY

Course Code : AID735PE

Question Number	List of Questions	Bloom's Taxonomy Levels
1	**A college online exam system was hacked, and the attacker:** 1. Read confidential question papers. 2. Changed some student marks. 3. Blocked the exam portal for 2 hours. **Identify these three attacks by name (Confidentiality, Integrity, Availability).**	BTL-2
2	Encrypt the plaintext **"DATA"** using a Caesar Cipher with shift = 3. Then decrypt it back.	BTL-3
3	Use the **2×2** Hill cipher with key matrix $K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$ to encrypt the plaintext **"MEET"** (use the mapping **A=0, B=1, ..., Z=25** and group letters in pairs). Then, using K^{-1}, decrypt your ciphertext to recover the original text.	BTL-3
4	AES can use keys of **128, 192, or 256 bits**. If AES-128 is used, calculate the total number of possible keys.	BTL-5
5	RSA system uses: $p = 5, q = 11, e = 3.$ Find modulus n, $\varphi(n)$, private key d, and encrypt the message $M = 9$.	BTL-6

Actual Date of Submission : 01.09.2025
Last Date of Submission : 06.09.2025