**COMSAT UNIVERSITY ISLAMABAD ATTOCK CAMPUS**

****

**INFORMATION SECUIRITY**

**NAME:** M USMAN SIDDIQUE

**REGISTRATION NO:** SP24-BSE-024

**LAB MID TERM**

**SUBMITTED TO:** Ms. AMBAREEN GUL

**DEPARTMENT:** SOFTWARE ENGINEERING

**DATE:** 20th October 2025

**Question 01: Caesar Cipher  
Code: A screen shot of a computer program

AI-generated content may be incorrect.**

**OUTPUT:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**QUESTION 02: Vigenère Cipher (Encryption Only)**

**CODE:   
A screen shot of a computer program

AI-generated content may be incorrect.**

**OUTPUT:**

**A screenshot of a computer program

AI-generated content may be incorrect.**

**QUESTION 03: Debugging Task (Simple XOR Encryption)**

**CODE:**

**A screen shot of a computer program

AI-generated content may be incorrect.**

**OUTPUT:**

**A screen shot of a computer

AI-generated content may be incorrect.**

**QUESTION 04:**

1. **DES vs AES:** DES is a 16-round Feistel cipher on 64-bit blocks with an effective 56-bit key; AES (Rijndael) is a substitution-permutation network (SPN) on 128-bit blocks, with 10/12/14 rounds for 128/192/256-bit keys, using steps like SubBytes, ShiftRows, MixColumns, AddRoundKey.
2. **AES block size**: 128 bits.  
   **One AES key size**: 128 bits (others are 192 and 256).
3. **Why AES is more secure**: **ChatGPT said:** AES uses far larger keys than DES - 128/192/256-bit vs DES’s 56-bit - so brute-forcing AES is computationally infeasible, while DES can be cracked with specialized hardware.