ISEC 2000 Fundamental Concepts of Cryptography
Lab 2
@ Computing, Curtin University

Notes:

- Make sure you complete prac questions. Assignments are highly related to them. In fact, programming questions are building blocks for the assignments.
- Group discussion is encouraged but make sure you complete questions individually.
- Ask questions not just answers. There is no answer of prac questions documented or provided for computing units.
- You can use your preferred programming language, C/C++, Java, or Python. Do NOT rely on libraries excessively.

1. Prove that $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$.

2. In Caesar cipher, is there a key such that we can recover the plaintext by applying encryption twice, i.e., $E_k(E_k(m)) = m$?

3. Please write a program to implement the Caesar cipher. It should consist of both encryption and decryption functions, which take the message (plaintext or ciphertext) and key as input and output encrypted or recovered message. Use your cipher to encrypt the message "attack at dawn" and then decrypt the ciphertext.