CSD451: Applied Cryptography
Assignment 1: Classical Cryptosystems

Date: September 3, 2023

Submission Guidelines:

- This assignment contains two problems. Each problem is of 5 marks.
- To submit the Assignment, upload the file to Blackboard.
- Email/paper submissions will not be accepted.
- Assignment submitted after due date will not be evaluated and a score of zero will be awarded for the assignment.
- Due date: **11:59 pm, September 10, 2023.**

Problem1: Implement the attacks described for the shift cipher and the Vigenère cipher. Your code should take a ciphertext as input and output the key alongwith the plaintext.

Problem 2: The shift cipher can also be defined over the 128-character ASCII alphabet (rather than the 26-character English alphabet).

a. Provide a formal definition of the scheme in this case.
b. Discuss how the attack we have studied can be modified to break the modified scheme.