

CSCI 476: Computer Security—Assignment 1 (6 marks)

This assignment is on building some hand-on experience with security and cryptography. It is recommended that you try to solve this problem using both programming and non-programming skills. It is highly recommended that you find some fellow students to form a 2- or 3-person group.

Background. Bob is a computer programmer and he found recently that somebody was investigating his background. He intercepted the corresponding email exchanges but unfortunately they are encrypted in some way. The only thing he knows is that the method of encryption is based on letter exchanges, e.g., exchange **a** with **z**, **b** with **w**, etc. But he doesn't know the actual key (i.e., which letter **a** is exchanged with, etc). In the emails, all letters are lowercase and all non-letter characters are intact (e.g., a space or a comma is left as is). Bob decided to do something to discover the contents of these email exchanges, which is put together into a text file `input.txt`. Unfortunately, Bob knows little about security and he needs your help to uncover the contents of this file, at least some of them.

Requirement. You should try to decrypt `input.txt` into something readable or half-readable. (The method is left open, you could try a combination of coding and Jeopardy-like game playing.) To finish the assignment, you need to answer the following questions:

1. How many kids does Bob have?
2. What modern programming language can Bob code in?
3. What is Bob's favorite pet animal?

Date Due: 11:30pm on Thursday, January 24, 2019 (on or before 11:30pm, Jan 24, 2019). Load your output as a separate file on D2L in the folder **Assignment 1**, preferably in the form of **family_name.output**. If you form a group with some fellow students (with at most 3 students in each group), only one of you needs to submit your solution and all of you will get the same mark.