Homework 1

Due: Thursday, April 7 at 12PM (noon).

You may discuss the problems in general terms in a group of size at most three. You are expected to write up your solutions yourself. Please credit your collaborators on your submission. You may use your course notes and slides to solve these problems.

You may use your course notes and slides to solve these problems.

Your Gradescope submission should include two files. The first is a write-up of your solutions; this may be either a PDF compiled from LaTeXor a PDF scan of handwritten work. Please name it `hw1.pdf`.

The second is a file containing any code that you used to solve Problem 2. Code will not be run for correctness but may be useful for partial credit. You may use any reasonable file names.

Problem 1 [10 points] Let $\mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$. Consider the symmetric encryption scheme in which a message $M = M[1]M[2]M[3]M[4] \in \mathbb{Z}_{10}^4$ is a four-digit string, a key $\pi \xleftarrow{\$} \text{Perm}(\mathbb{Z}_{10})$ is a random permutation on $\mathbb{Z}_{10}$, and the ciphertext $C = C[1]C[2]C[3]C[4] = \mathcal{E}_\pi(M) \in \mathbb{Z}_{10}^4$ is computed as follows:

Alg $\mathcal{E}_\pi(M)$
For $i = 1, \ldots, 4$ do
  $P[i] \leftarrow (M[i] + i) \bmod 10$
  $C[i] \leftarrow \pi(P[i])$
Return C

(a) **[2 points]** Specify a decryption algorithm $\mathcal{D}$ such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme (Lecture 2 Slide 2) meeting the correct decryption requirement (Lecture 2 Slide 4).

(b) **[4 points]** Is this scheme a substitution cipher as per the definition of Lecture 2 Slides 10, 11? Why or why not?

(c) **[4 points]** Is this encryption scheme perfectly secure as per the definition of Lecture 2 Slide 39? Why or why not?

Problem 2 [10 points] For this problem, solve by hand or write a program (perhaps in Python). If you write a program, please submit the code as a second submission file, as described above.

This problem involves cryptanalyzing a *Vigenère cipher*, which you may read about on Wikipedia: `https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher`. Vigenère ciphers can generally be deciphered using Kasiski examination, which is discussed on the Wikipedia page.

You can find some ciphertext produced with the Vigenère cipher under a certain key on our course website at: `https://cseweb.ucsd.edu/classes/sp22/cse107-a/resources/hw1/ciphertext`.

We have also provided sample decryption code at:
`https://cseweb.ucsd.edu/classes/sp22/cse107-a/resources/hw1/decrypt.py`.

Encrypting a plaintext letter with a key letter `A` results in no change, encrypting with a key letter `B` results in an increment by one place in the alphabet, encrypting with a key letter `C` results in an increment by two places, and so on. Assume that the original plaintext contains only uppercase letters (`A-Z`) and no spaces or punctuation.

For example, encrypting the plaintext `ATTACKATDAWN` with the key `BLAISE` results in the following ciphertext:

Plaintext	`ATTACKATDAWN`
Key	`BLAISEBLAISE`
Ciphertext	`BETIUOBEDIOR`

The goal for this part of the homework is to figure out what key was used to encrypt your ciphertext.

(a) **[4 points]** What is the key? (For partial credit, what is the length of the key?)

(b) **[6 points]** How did you recover the key? Explain your methodology at a high level. Feel free to reference sections of your submitted code, but please write your explanation in clear English sentences.
