CS 198 Codebreaking at Cal
Spring 2023 Makeup Assignment

Week 10

Question 1

Suppose we define an encryption function $E(K,M) = KM$ (where K is a key and M is a message, both represented as integers). (This is probably not a very secure encryption scheme!)

1. Is this scheme additively homomorphic?
2. Is this scheme multiplicatively homomorphic?

Question 2

The CS 171 staff are competing to see who can write the hardest midterm question, but they don't want to reveal their questions to each other yet. Suppose each question can be uniquely represented as an integer based on its difficulty (harder questions correspond to higher integers). Each staff members has a key K, and they all have access to a fully homomorphic encryption function $E(K,M)$ (where K and M are both integers).

Design a scheme so that they can find out who wrote the hardest question without anyone revealing their questions. (You don't need a technical specification, just a few sentences of a high-level overview).

Contributors:

- Ryan Cottone, Will Giorza