CS 198 Codebreaking at Cal
Spring 2023 Makeup Assignment

Week 6

Question 1

Alice and Bob don't like modular arithmetic, so they decide to do a Diffie-Hellman key exchange but work over real numbers instead of a modulus. Why is this a bad idea?

Question 2

What is the order of 3 (mod 7)?

Question 3

Suppose we had an algorithm that could factor an integer n and ran in $O(\sqrt[9999]{n})$. In terms of the *number of bits* in n, would this algorithm run in exponential or polynomial time?

Question 4

Use Pollard's Rho algorithm to factor 2149, and write out the value of x, y, and d at each step. (You should find a factor after a very small number of steps.)

Contributors:

- Ryan Cottone, Will Giorza