CS 198 Codebreaking at Cal
Spring 2023 Homework

HW 9

Question 1

Briefly explain why quantum computers pose a threat to cryptography.

Question 2

Let $L \subset \mathbb{R}^2$ be the lattice given by the basis $v_1 = (213, -437)$ and $v_2 = (312, 105)$ and let $w = (43127, 11349)$.

HINT: We recommend doing Lab 9 before doing these questions, as the functions there can help with the computational parts of this problem.

1. Use Babai's algorithm to find a vector v that is close to w. Compute the distance $\|v - w\|$.
2. What is the Hadamard ratio of this basis? Do you think this represents a good basis or a bad basis?
3. Show that the vectors $v_1' = (2937, -1555)$ and $v_2' = (11223, -5888)$ are also a basis for L by finding the unimodular matrix U that transforms $\{v_1, v_2\}$ into $\{v_1', v_2'\}$. Recall that a unimodular matrix is one with integer entries and a determinant equal to 1. *HINT: Setup a system of linear equations and solve.*
4. Use Babai's algorithm to find a short vector v' that is close to w using this new basis. Compare the norm of this vector to the one you found in part a).
5. Compute the Hadamard ratio of this new basis, and conclude whether or not $\{v_1', v_2'\}$ is a good basis.

Contributors:

- Ryan Cottone