CS 198 Codebreaking at Cal
Spring 2023 Makeup Assignment

# Week 9

## Question 1

Explain why public-key encryption is more vulnerable to attacks with quantum computers than symmetric encryption.

## Question 2

Suppose we have a lattice determined by the basis vectors $(3,1)$ and $(4,1)$.

1. What is the shortest vector in this lattice? (*Hint: try drawing it out*)
2. What is the area of this lattice's fundamental domain?

## Question 3

Suppose Alice wants to send a message to Bob using GGH. Bob uses the lattice determined by the basis $(1,1)$ and $(1,-1)$ (his private basis vectors). He reveals $(171,171)$ and $(171,161)$ as his public key.

Alice sends Bob the ciphertext $(50.3,9.6)$.

1. What should Bob decrypt the message to?
2. How could another observer, Eve, decrypt the message?

**Contributors:**
- Ryan Cottone, Will Giorza