Welcome to Homework 19!

These questions are largely conceptual. The notebook will help you build a strong intuition and understanding of the concept but is not necessary to answer these questions.

1. **Why is a key necessary in secure communication?**

A) A key is special in that it cannot be intercepted during transfer
B) A key lets the receiver measure the sender's qubits.
C) A key can allow the sender to encrypt and the receiver to decrypt coded messages

2. **Why is QKD secure?**

A) The transfer of key is the most vulnerable point of creating a secure channel, QKD utilizes quantum mechanics to alert the sender and receiver if the key has been intercepted during transport with a high probability.
B) QKD uses quantum teleportation to send messages so the message instantly goes to the receiver.
C) The only way to break QKD encryption is with another Quantum computer.

3. **What would happen if Eve tries to intercept Alice's key on its way to Bob?**

A) Bob will never receive the qubit and will know that Eve intercepted it.
B) Bob and Alice will have different results when comparing the first few bits of their key and will know that Eve intercepted the key.
C) Bob will be able to tell that his qubits have been measured and will know that Eve must have intercepted them.

4. **True or False: Alice needs to send physical qubits in the QKD protocol?**

A) True: The qubit is what Bob will measure.
B) False: Alice only needs to send classical bits.

5. **True or False: Every message that Alice and Bob send after successfully generating a key using QKD needs to be sent over the quantum channel if they want keep their messages secure.**

A) True: Classical messages are by nature insecure.
B) False: Once they have a key, they can use encryption to keep the messages safe.