CS333 - Problem Set 2

1. In your own words, describe what it is about quantum states that makes it possible for Alice and Bob to share a secret key over a public channel (a public channel is a channel where eavesdropping is possible).

2. Read The Space-Based Quantum Cryptography Race and explain (1) why scientists are trying create a quantum cryptography satellite and (2) given your understanding of the BB84 quantum cryptography protocol, why is it important that the error rate is below some threshold. (You don't need to explain the 11% in particular, just why some threshold should exist.) (Update if you are interested: the Chinese satellite has been launched and was used to hold a secure video conference. See Chinese satellite uses quantum cryptography.)

3. Suppose Alice sends Bob a photon that is either vertically, horizontally, right-diagonally, or left-diagonally polarized. Suppose Bob puts a vertically polarized filter in front of a single photon detector. If Bob's detector's light turns on, what does he know for sure about the polarization of the photon Alice sent? If the detector's light does not turn on, what does he know for sure about the polarization of the photon Alice sent? Please explain.

4. Suppose Alice sends a vertically polarized photon through a diagonally polarized filter, followed by a vertically polarized filter. What is the probability that a photon will exit the second filter, and if one does exit, what will its polarization be after exiting?

5. Consider the following strategy for Eve: she chooses to intercept and measure each photon Alice sends with probability p, (with probability $1-p$ she lets the photon go through untouched to Bob). When she does measure, she always measures using a vertically polarized filter, and then passes on a vertically or horizontally polarized photon based on the outcome of her measurement: she sends a vertically polarized photon if she detects a photon exiting her filter, and she sends a horizontally polarized photon if she does not detect a photon. If Alice and Bob follow the same protocol as described in class, what is the probability that a bit of b' will differ from the corresponding bit in d'?