CS333 - Problem Set 1

1. If you haven't yet, do the Math Practice worksheet.

2. Consider a message m that consists of one bit, so $m \in \{0,1\}$, and a secret key $s \in \{0,1\}$. Using the XOR encryption from class, create a table that shows what $\overline{m}$ is for every possible message/key combination. Use this table to argue that Eve can not determine m from $\overline{m}$ if she knows nothing about the value of m or s. (You may also use Baye's rule, if you know it, but this is not necessary.)

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 what will its polarization be after exiting?

5. If Eve chooses to measure a photon Alice is sending to Bob with probability p, and 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, what is the probability that a bit of b' will differ from the corresponding bit in d'? Assume Alice's and Bob's strategy is the same as in class.

6. **Not due this week!!! Will be due as part of next week's assignment.**
   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).

7. **Not due this week!!! Will be due as part of next week's assignment.**
   Read The Space-Based Quantum Cryptography Race and explain (1) why scientists are trying create a quantum cryptography satellite and (2) why is it important that the error rate is below some threshold. (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.)

8. How long did you spend on this homework?