Pre Lab Exercise #1: Fill in the table below.

Alice's Message (ascii)	Q								K								D							
Alice's mess. (binary)	0	1	0	1	0	0	0	1	0	1	0	0	1	0	1	1	0	1	0	0	0	1	0	0
OTP (binary)	0	0	1	0	0	0	1	0	1	1	0	1	1	0	0	0	1	0	0	1	1	0	1	0
Encrypted mess.	0	1	1	1	0	0	1	1	1	0	0	1	0	0	1	1	1	1	0	1	1	1	1	0
OTP (same as above)	0	0	1	0	0	0	1	0	1	1	0	1	1	0	0	0	1	0	0	1	1	0	1	0
Bob's mess., binary	0	1	0	1	0	0	0	1	0	1	0	0	1	0	1	1	0	1	0	0	0	1	0	0
Bob's message (ascii)	Q								TC K								TC D							

Pre Lab Exercise #2:

(a) *Complete the table below for an n = 2 protocol,* $\delta = 2$. If Bob's measurement outcome is unknown, put in a "?". The state sent should be one of (H , V, +, -).

Alice's key a	*Alice's basis choice b*	*State sent*	*Bob's basis choice b'*	*Bob's a'*
0	**+/-**	+	**H/V**	**?**
1	**+/-**	-	**+/-**	**1**
1	**+/-**	-	**H/V**	?
1	**H/V**	V	**H/V**	1
1	**+/-**	-	**H/V**	?
0	**H/V**	H	+/-	?
1	**H/V**	V	+/-	?
0	**+/-**	+	+/-	0
1	**+/-**	-	**H/V**	?
0	**H/V**	H	**H/V**	0

(b) What is the final key that Bob and Alice share?

1100 TC

Pre Lab Exercise #3:

(a) Complete the table similar to Exercise #2, however, with Eve as an interceptor. If Bob's outcome is uncertain, put in a "?". Like Bob, Eve will also be uncertain but must always resend a photon to minimize suspicion.

Bit #	*Alice's key a*	*Alice's basis choice b*	*Eve's basis choice*	*Eve's intercepted message*	*Eve's resend basis*	*Bob's basis choice b'*	*Bob's a'*
1	**0**	+/-	**H/V**	**1**	**H/V**	**H/V**	1
2	**1**	**H/V**	+/-	**0**	+/-	+/-	0
3	**1**	+/-	**H/V**	**1**	**H/V**	**H/V**	1
4	**1**	**H/V**	+/-	**0**	+/-	**H/V**	?
5	**1**	+/-	+/-	**1**	+/-	+/-	1
6	**0**	**H/V**	+/-	**0**	+/-	**H/V**	?
7	**1**	**H/V**	**H/V**	**1**	**H/V**	+/-	?
8	**0**	**H/V**	+/-	**0**	+/-	**H/V**	?
9	**1**	+/-	+/-	**1**	+/-	+/-	1
10	**0**	**H/V**	**H/V**	**1**	**H/V**	+/-	?

(b) What bit numbers will Alice and Bob keep after communicating?

4,5,6,8,9 TC

(c) What is Alice's final bit string? What is Bob's? What is the probability that Eve did not produce one error?

Alice's final string: 1 1 0 0 1
Bob's final string: ? 1 ? ? 1

Eve produces an error whenever Bob and Alice have the same basis as each other but Eve has a different basis. P(B=A) = .5, so P(B=A\=E)= 1/4. So the probability that eve does not produce an error is 3/4. TC

(d) If Alice sends a string of photons of length (N), with Eve intercepting and resending EVERY photon, what is the probability, as a function of N, that Eve does NOT produce an error?

(3/4)^N TC

(e) Why should Eve choose her measurement basis at random?

The probability in (d) is maximized for when Eve choses their measurement at random, such that they are most likely to have the same basis as both Bob and Alice. TC

(f) Why won't it work for Eve to make a copy of the photon and then measure it AFTER Alice and Bob have classically communicated which bits to keep?

Even if Eve knows which bits are being kept, they do not know which basis is being used for each bit by Bob and Alice. TC

Pre Lab Exercise #4:

(a) What value of λ gives the highest possible probability of getting k=1 photon per pulse? What is that probability $P_{k=1}$ in this case? $\frac{d}{d\lambda}P = -\lambda e^{-\lambda} + e^{-\lambda} \Rightarrow \lambda = 1 \Rightarrow \frac{1}{e} = P$ TC

(b) What's the probability of k=0 and k>1 with the λ in part (a)? What are the ratios of $P_{k=0}$: $P_{k=1}$ and $P_{k>1}$: $P_{k=1}$ in this case?

1/e: the ratio of the probabilities is 1. TC

(c) What is the probability of getting 1 photon if the probability of >1 photon in this case is <1%? (Hint: find λ first.) What are the ratios of $P_{k=0}$: $P_{k=1}$ and $P_{k>1}$: $P_{k=1}$ in this case?

The ratios of both are still 1/e

Pre Lab Exercise #5: Consider another way to use the photons to generate random numbers and explain.

Send photon pulses of Horizontally polarized light through a HWP rotated by 22.5 degrees. This will produce light in the state |+> = 1/sqrt2 (|H> + |V>). Now measure |H> and |V> (using a PBS). Record |H> incidences as 0 and |V> as 1.