A. Consider the basic Bennett (1992) key exchange protocol with no eavesdroppers and no errors in the communications channels. Verify the claim that I eventually made that, in each iteration of the protocol, the probability of Ariko and Babatope successfully agreeing on a bit value is 1/4.

B. I've laid out a possible strategy for the eavesdropper Einar. And I've drawn out the left side of a big tree illustrating the probabilities of various subcases. Draw out the right side of the tree, checking your results against my claims about the failure rate, false success rate, and true success rate.

C. In Bennett's algorithm, Ariko encodes $|0\rangle$ and $|1\rangle$ into $|0\rangle$ and $|+\rangle$, respectively. You might wonder whether it possible to build a similar cryptosystem where $|0\rangle$ and $|1\rangle$ are encoded into some other fixed states $|\chi\rangle$ and $|\omega\rangle$, respectively. So here's my question: Why would it be a bad idea to use $|\chi\rangle$ and $|\omega\rangle$ such that $\langle\chi|\omega\rangle = 0$?