As far as I know, Bennett's algorithm is not safe against "man-in-the-middle" attacks. If Einar can completely intercept all communications between Ariko and Babatope, then he can wait for Ariko to initiate the protocol, set up a key with her, set up a separate key with Babatope, and relay information between them, reading it along the way. In general cryptography, you prevent this attack using some kind of authentication. I don't know how that's supposed to work here, and maybe no one does, and anyway it would take us too far astray from this course's core material. But the following exercise discusses one kind of man-in-the-middle attack.

A. Suppose that Einar has some ability to intercept the communications between Ariko and Babatope. Here's his plan. He intercepts $|\psi\rangle$ and measures it, thereby obtaining either $|0\rangle$ or $|1\rangle$. If he sees $|1\rangle$, then he sends $|+\rangle$ on to Babatope. If he sees $|0\rangle$, then he rolls a six-sided die. If he rolls a 1, 2, 3, or 4, then he sends $|0\rangle$ on to Babatope. If he rolls a 5 or 6, then he sends $|+\rangle$ on to Babatope. So Babatope receives $|0\rangle$ or $|+\rangle$, as in the algorithm without eavesdroppers, but he doesn't know that it's coming from Einar. Meanwhile, Einar has extracted some information, which might help him decrypt subsequent messages between Ariko and Babatope.

The question is: Can Ariko and Babatope detect Einar's interference? How, exactly? Be thorough. You should probably draw a tree describing the cases.

This next exercise is much, much shorter (once you see the answer, at least). The ideal answer is simple and precise.

B. In Bennett's algorithm, Ariko encodes $|0\rangle$ and $|1\rangle$ into $|0\rangle$ and $|+\rangle$, respectively. You might wonder whether it's possible to build a cryptosystem where $|0\rangle$ and $|1\rangle$ are encoded into some other fixed states $|\chi\rangle$ and $|\omega\rangle$, respectively. (To clarify, everyone in the world would know what $|\chi\rangle$ and $|\omega\rangle$ are. The cryptosystem itself is public information.)

So here's my question: Suppose, as in the previous exercise, that Einar has the ability to intercept $|\psi\rangle$, do things to it, and pass on a new state to Babatope. Why would it be good for Einar, if Ariko and Babatope used $|\chi\rangle$ and $|\omega\rangle$ such that $\langle\chi|\omega\rangle = 0$?

This last question is optional. It's phrased in an open-ended way, but there is a fairly narrow correct answer.

C. The previous exercise shows that some choices of $|\chi\rangle$ and $|\omega\rangle$ are terrible. Is Bennett's choice of $|\chi\rangle = |0\rangle$ and $|\omega\rangle = |+\rangle$ optimal? Or are there better choices? More basically, what even makes one choice better than another?