Marking H1A

First submission:

1. Nice and clear explanation. You are explaining the use of the multiplicative property of RSA and showed examples - 1
2. ?
3. Simple answer that is easy to understand - 1
4. You explain a lot regarding how the CVV1 doesn't work against skimming, but there you don't mention which attack it prevent other than telling us where the CVV1 is located. – 0.8
5. You explain the first question. But never really answer the questions: "What would differ if CA signs the card's secret key instead?" – 0.7
6. Good description for both advantage and disadvantage - 1
7. Long and detailed description. Could probably have been shortened to a simpler answer, but it's still good - 1
8. Good description of the cut-and-choose technique – 1

Second submission:

1. Nice and simple explanation – 1
2. The answer is maybe a little bit too simple. You never explain why it’s fully untraceable? Maybe mention how it’s untraceable is a good idea. Giving some pin-points to how the blind signatures is created/used and why the bank can’t trace it. 0.8
3. This is kind of related to the first question. In both the schemes mentioned in the lectures, Alice doesn’t need to send a signature. The point is that in the fully untraceable scheme, the bank doesn’t have a way of finding out the ID of the owner of the coin, as it is never included during the withdrawal or the use of the coin.