A-1 In EMV, SDA cards are cards that only support SDA data authentication. List some advantages and drawbacks of these cards compared to cards that support DDA. Can you find an attack that would work on SDA cards but not on DDA compatible cards?

Grading: 1.0
Motivation:
The answer agrees with the information on for example this page:
https://www.scribd.com/doc/46386349/EMV-SDA-vs-DDA

A-7 Is SSL required in SET? Motivate your answer.

Grading: 1.0
Motivation:
Correct answer. Matches well with the information on the slides from "Electronic Payments, part 1".

A-9 In 3D Secure, describe briefly what happens after the Merchant/MPI receives the PARes from the issuer.

Grading: 1.0
Motivation:
Once again a correct answer. Could be a bit more detailed. The info corresponds with the slides "Electronic Payments, part 1" as well as: https://tech.dibspayment.com/DT/API/3d-secure_guide

A-13 What is the difference between authorization and authentication in VbV (3D Secure)?

Grading: 1.0
Motivation:
Well written answer. Besides common sense, information can be found here:
https://usa.visa.com/run-your-business/small-business-tools/payment-technology/verified-by-visa.html

A-17 How can the cut–and–choose technique be used to make sure that identifying information is properly added into an untraceable coin?

Grading: 1.0
Motivation:
It is a difficult question but the author did a good job. However, the answer is a bit messy. I would've preferred some mathematical formulas instead of plain text.

A-23 In PayWord, a unit could be, e.g., one cent (or one öre), so even though the payments are "micro", the hash chains could be pretty long. Could this pose a storage problem to Alice,

who has to generate the entire chain when (before) she makes her first purchase from a merchant?

Grading: 1.0
Motivation:
Good and clear answer. It agrees with the information on “Electronic Payments, part 2”.

A-28 Compare the PayWord protocol and the Peppercoin-like protocol in the lecture notes from the point of view of the customers, both in terms of what they pay, and in terms of what they need to compute to make a purchase.

Grading: 0.6
Motivation:
Never answers the question “what the pay”. The text about computing is however good and goes well with the slides in “Electronic Payments, part 2”.

A-30 Compare the anonymity given by the untraceable E-cash scheme and Bitcoin.

Grading: 0.8
Motivation:
Overall a good answer. However, there could have been said a bit more about how Bitcoin handles anonymity with private and public keys as well as addresses. The wikipedia page describes it very well: https://sv.wikipedia.org/wiki/Bitcoin.

Total score: 7.4