A-2 In ASN.1, what is the difference between implicit and explicit tagging?

Grading: 1.0
Motivation:
Good and clear answer. Nice with an example. The answer agrees with the information on the lecture slides (page 6).

A-5 Draw a tree based on the OBJECT IDENTIFIER id-sha256. Include some extra nodes that seem suitable/reasonable. Identify some arcs in your picture.

Grading: 1.0
Motivation:
The answer seems correct according to the lecture notes on page 4.

A-6 In ASN.1, what is the difference between DEFAULT and OPTIONAL?

Grading: 1.0
Motivation:
Once again a correct answer. Similar information can be found in the lecture notes on page 4.

A-7 Consider the example on page 10 in the lecture notes where PER requires only one octet to represent (a,b,c)=(a,b,(c1,c2,c3)), but DER requires several octets. Give both the DER encoding and the PER encoding for the case where (a,b,c)=(TRUE,30,(TRUE,FALSE,50)).

Grading: 0.0
Motivation:
I had the same question and couldn't answer it either.

A-24 With password integrity mode in PKCS #12, the MAC is computed over encrypted data. Another strategy could be to compute the MAC over the plaintext and then apply encryption (including or excluding the MAC). In general, which variant to use is chosen by protocol or algorithm designers. How is it done in SSL?

Grading: 1.0
Motivation:
Correct. I found a similar conclusion on this page for example:
https://crypto.stackexchange.com/questions/202/should-we-mac-then-encrypt-or-encrypt-then-mac

A-25 Compare the support for Proof of Possession in PKCS#10 and CRMF

Grading: 1.0
Motivation:

A well-put answer. It agrees with the information on the lecture notes (page 16-18).

A-27 Can a DoS attack stop a CRL update from reaching a potential victim? How should that victim behave when the nextUpdate time has been reached and no update has arrived?

Grading: 1.0
Motivation:
Correct. The answer agrees with the lecture notes and these pages:
https://searchsecurity.techtarget.com/definition/Certificate-Revocation-List
https://www.xolphin.se/support/Terminologi/Certificate_Revocation_List_(CRL)

A-31 Describe a sensible replay attack in OCSP. What could it accomplish? How does the protocol deal with replay attacks?

Grading: 1.0
Motivation:
Good answer. It agrees with the information in the lecture notes (page 24) and on the wiki page:
https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

Total score: 7.0