A-4 In ASN.1, describe the difference between SET and SEQUENCE and explain why one is usually the better choice.

Grading: 1.0
Motivation:
Correct answer. Agrees with the information on the lecture notes on page 2-3.

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 tree looks correct according to the lecture notes.

A-12 Is DER and CER always valid BER? Explain.

Grading: 1.0
Motivation:
True. Corresponds to the information in the lecture notes on page 9 for example.

A-14 Give the DER encoding of the INTEGER 10000 (ten thousand)

Grading: 1.0
Motivation:
Correct once again! I got the same encoding.

A-16 In CMS, there is a Signed-Data type as well as an Encrypted-Data type. Intriguingly, there is no Signed-Encrypted-Data type, although it is no doubt useful to encrypt and sign data (at the same time). Why is this?

Grading: 1.0
Motivation:
The answer could have been a bit more thorough. However, I couldn't really find any additional information, so I'll give you a maximum score.

A-20 Consider the SignedData type in CMS. The digestAlgorithms are given as a "SET OF DigestAlgorithmIdentifier". Since a "SET OF" does not have a particular order, how can we know which digest algorithm corresponds to which signer? Or do we not care?

Grading: 1.0
Motivation:
A very well-put answer. It is difficult to find an explanation in the lecture notes, but your answer is very reasonable.

A-26 For digital signatures, clearly explain an attack that would be possible if the Proof of Possession is not used in a certificate request

Grading: 1.0
Motivation:
Correct. I had the same question and gave a similar answer.

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:
Correct answer. Agrees with the information on the lecture notes (page 24) and on the Wikipedia page: https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

Total score: 8.0