Home Assignment 5

Rasmus Olofzon, 9104192472

Complete the eight A-assignments below and solve them individually.

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

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

A-13 In ASN.1, an INTEGER has tag value 0x02, which is BER encoded to 0x02. A SEQUENCE has tag 0x10, which is BER encoded to 0x30. Explain the discrepancy.

A-17 For signed-data in CMS, several signers can sign the same data. How is this feature achieved?

A-18 Give an example of multiple representation of the same data in CMS. Motivate this redundancy.

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?

A-23 In PKCS #12, assume that we want to represent a private key. It should be privacy and integrity protected using a password. What is the minimum number of ContentInfo types we have to define in order to produce a valid PFX? Which are the ContentTypes we should use?

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?