Home Assignment 5

Niklas Jnsson, 9208273772

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

A-1 In the lecture notes, the type Course has been imported from the LTH-module. Write a suitable definition of this type. You must use at least three different types in your definition.

A-8 For each of BER, CER, DER, PER, and XER, give the full name and summarize the main idea behind that particular encoding rule.

A-9 For the long definite form, what appears to be the maximum length possible to encode?

A-11 Decode the following: 3A 82 00 10 1A 01 73 1A 02 65 63 1A 81 06 75 72 69 74 79 21. What encoding rule is it?

A-19 Consider the SignedData type in CMS, which is used to sign data. Where is the actual signed data (e.g., a document, a letter or a contract) given?

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-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?