1. **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.**

   ```
   Course ::= SEQUENCE {
       courseCode      VisibleString,
       institution     UTF8String
       teachers     SEQUENCE OF SEQUENCE {
           name      UTF8String
           phone      SEQUENCE OF SEQUENCE {
               phoneID      VisibleString
               number      NumericString
           }
       }
   }
   ```

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

   Implicit tagging means that the universal tag is replaced by the context-specific tag.

   Explicit tagging instead adds an outer tag environment in addition to the original tag.

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

   DEFAULT is for giving a types a default value.

   OPTIONAL means that the value is optional and does not have to exist.

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)).**

   DER: 0x02 (SEQUENCE) 0x09 (length of everything) 0x01 (BOOLEAN) 0x01 (length of a) 0x0F (TRUE) 0x02 (INTEGER) 0x01 (length of b) 0x1E (30) 0x02 (SEQUENCE) 0x09 (length of c, 9 octets are following) 0x01 (BOOLEAN) 0x01 (length of c1) 0x0F (TRUE) 0x01 (BOOLEAN) 0x01 (length of c2) 0x00 (FALSE) 0x02 (INTEGER) 0x01 (length of b) 0x32 (50) This gives (in hexadecimal): 0x020901010F02011E020901010F010100020132.

   PER: TRUE is encoded as 1, 30 is encoded as 011 as $30 - 27 = 3$ and it can only assume 8 different values and 3 bits is enough, FALSE is encoded as 0 and 50 is encoded as 00 as the lowest allowed value is 50 and $50 - 50 = 0$ and would be 2 bits long as it can only assume values between 50 and 53. This gives (in bits): 10111000.

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

   In long definite form the first octet is used to describe how many following octets there are and one bit (MSB) is always set to one, this means that we can at most have 127 octets to describe the length. With 127 octets we get: $2^{8\cdot127} \approx 7.0 \cdot 10^{305}$, this would be the maximum length (in octets) possible to encode.

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

   The Signed-Data Type contains the SET OF SignerInfo, each of these SignerInfo types contain the signature and other data needed to check the signature. Since the signatures and other signature relevant data is stored in a separate type which in itself is stored in a SET OF type, one can simply add another SignerInfo to the SET OF SignerInfo if one would want to add another signature for the data.

7. **A-20 Consider the SignedData type in CMS. The digest Algorithms 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?**

   The used digest algorithms is stored in two different places, in the "SET OF DigestAlgorithmIdentifier" and in the SignerInfo sequences. Every signer has a SignerInfo and this defines which digest algorithm was used along with the other data needed to test the signature, such as the signature itself and which certificate's public key that are to be used and so on. The "SET OF DigestAlgorithmIdentifier" appears to be used if one wants to check all the signatures at once (so that one can hash the data first and then use that to check all the signatures in one go).

8. **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 single ContentInfo should be enough as we only want to store a single key.

   The ContentType PKCS8ShroudedKeyBag should be used as it can store an encrypted private key.