Home Assignment 5
EITN41

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

Answer: In implicit tagging the class is context-specific. The universal tag is replaced by a context-specific tag. In explicit tagging the class needs an outer tag environment (in addition to the original tag) in order to be sufficiently specified.

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

Answer: `DEFAULT` lets one specify a default value for a type. `OPTIONAL` can be used to define a value that is optional and does not have to exist.

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.*

Answer: It has to do with *Primitive* and *Constructed* types. A Primitive type means that the value is the actual value of the type, and a Constructed type means that the value is itself a series of TLV (Type-Length-Value) encodings. The `P/C` bit in an identifier byte specifies the type (0 for primitive and 1 for constructed). A `BOOLEAN` is just a value, hence a Primitive type, and its identifier byte will give 0b0000 0000 (00 in the beginning because a `BOOLEAN` is a universal class). A `SEQUENCE` will be a constructed type, hence the identifier byte will be 0b0011 0000, which is 0x30. That is why there is a discrepancy.

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

Answer: It is achieved with the `signerInfo` field of the `SignedData` type. In it, a `SET OF SignerInfo` describes the signers of the data and things like the algorithm used (`signatureAlgorithm`), their CMS version (`version`) and their signature (`signature`).

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

Answer: Here the six types of data is intended, i. e. Data Type, Signed-Data Type etc. Note that the Data Type usually is embedded in one of the other five data types.

The motivation for these different types are that data needs to be represented in different ways in different ways in different protocols, and this facilitates that.

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?*

Answer: As mentioned in A-17, the signatures are "stored" in a type `SignerInfo`. Here, each signature is mapped to a signer's identity (`SignerIdentifier`). Therefore, it does not matter that a `SET` is unordered, because a mapping between signed data and signer is included in the `SET`.

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?*

Answer: This corresponds to Password Integrity Mode. We should use a `Data Type` inside an `Encrypted-Data Type` inside a `Digested-Data Type` or a `Authenticated-Data Type`. So, a number of three (3) ContentTypes.

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?*

Answer: -