Home Assignment 5

A-3 It is possible to constrain the types when writing the ASN.1 specification, e.g., to specify that an integer can only take a certain number of values. Why is this important when using PER as encoding rules?

The purpose of PER (Packed Encoding Rules) is to encode using as few bits as possible. If we for example want to transmit a boolean value, only one bit is sufficient (1 for true and 0 for false for example). So instead of wasting 8 bits, we can limit the number of bits to 1. PER can be used when space is limited. The lecture notes mentions smart cards as an example.

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)).

...

A-10 One BER encoding of the VisibleString "string" is given by 3A 80 1A 03 73 74 72 1A 03 69 6e 67 00 00 as can be seen in the lecture notes. Change this encoding so that short definite form is used for the outer TLV. Do not change the fragmentation.

...

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?

"security!"
BER is used.

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

Yes. BER is more flexible than DER and CER who in turn place more restrictions on the sender. The X.690 standard states that: "Alternative encodings are permitted by the basic encoding rules as a sender's option. Receivers who claim conformance to the basic encoding rules shall support all alternatives."

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.

It is due to SEQUENCE type being *constructed* while INTEGER is *primitive*. A constructed type is not encoded according to the actual value but rather a series of TLV encodings.

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

Each signer retrieves a message digest and hash value for the data. Then, the message digest is signed using each of the signer's private key. The signature value is collected for each signer and stored in the SignerInfo value. Finally, all the message digest algorithms, SignerInfo values and data are collected and stored in the SignedData value. In the normal case, if a recipient can validate one of the signatures, the overall verification is successful.

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.

If the Proof of Possession is not used, an adversary can get a certificate from a CA for a given public key corresponding to a user. The adversary can then claim that he or she is the legitimate signer of a message. It is not possible for us to know if the claim is true or not, that is if the claim comes from the real user or the adversary.