Connect to **aisa.fi.muni.cz** using Putty or ssh, with **xlogin** and faculty password

Use WinSCP to copy **copy_to_aisa.zip** to your **home/local** (if no local there create using **mkdir**).

Change directory	**cd ~/local**
Unzip with:	**unzip copy_to_aisa.zip**
Change access permissions:	**chmod 777 asn1-install.sh**
Install compiler with:	**./asn1-install.sh**
Try	**asn1c -help**

Or install on your laptop from: https://github.com/vlm/asn1c

View ASN.1 structure of a file:

See the content of a certificate **in Practice/copy_to_aisa/asn1c-working/csca.der:**

```
openssl x509 -text -noout -inform DER -in csca.der
```

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 1 (0x1)
      Signature Algorithm: 1.2.840.113549.1.1.10
      Issuer: C=CZ, O=Czech Republic, OU=Ministry of Interior, CN=CSCA_CZ
      Validity
         Not Before: Jul 24 00:00:00 2006 GMT
         Not After : Oct 24 23:59:59 2021 GMT
      Subject: C=CZ, O=Czech Republic, OU=Ministry of Interior, CN=CSCA_CZ
      Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (3072 bit)
      Modulus (3072 bit):
```

Convert certificate from DER to PEM:

```
openssl x509 -out csca.pem -inform DER -in csca.der
```

Prepare the C and H files for the ASN.1 structures:

```
asn1c sod.asn1
```

```
Compiled AlgorithmIdentifier.c
Compiled AlgorithmIdentifier.h
Compiled LDSSecurityObjectVersion.c
Compiled LDSSecurityObjectVersion.h
Compiled DigestAlgorithmIdentifier.c
Compiled DigestAlgorithmIdentifier.h
```

Compiled LDSSecurityObject.c
Compiled LDSSecurityObject.h
Compiled DataGroupHash.c
Compiled DataGroupHash.h
Compiled DataGroupNumber.c
Compiled DataGroupNumber.h
Symlinked /usr/local/share/asn1c/ANY.h -> ANY.h
Symlinked /usr/local/share/asn1c/ANY.c -> ANY.c
Symlinked /usr/local/share/asn1c/INTEGER.h -> INTEGER.h
Symlinked /usr/local/share/asn1c/NativeEnumerated.h -> NativeEnumerated.h
Symlinked /usr/local/share/asn1c/INTEGER.c -> INTEGER.c

Compile a sample application:

Remove converter_example.c: **rm converter_example.c**
Compile: **gcc *.c -o LDSview -I. -DPDU=LDSSecurityObject**
And execute: **./LDSview**