[toc]

# 课上测试

## ch03

### 作业题目：DER编码

完成下面任务（9分）

1. 在 Ubuntu 或 openEuler 中完成任务（推荐openEuler）
2. 使用抽象语法记法（ASN.1）来定义学生数据结构： StudentInfo ::= SEQUENCE { studentID INTEGER, name IA5String, score INTEGER }
3. 对上面数据结构使用你的信息进行填充，studentID是 8 位学号；name 是姓名首字母；score：60-100 数字，填充完使用 echo 命令得到“你的八位学号.der”文件，给出编码过程和echo命令具体内容（5 分）
4. 使用 od 命令查看“你的八位学号.der”文件的内容，提交运行结果（2分）
5. 使用 OpenSSL asn1parse 命令解析“你的八位学号.der”文件，提交运行结果（2分）

**作业提交要求 (1')**

0. 记录实践过程和 AI 问答过程，尽量不要截图，给出文本内容
1. (选做)推荐所有作业托管到 gitee或 github 上
2. (必做)提交作业 markdown文档，命名为“学号-姓名-作业题目.md”
3. (必做)提交作业 markdown文档转成的 PDF 文件，命名为“学号-姓名-作业题目.pdf”

- github链接

**作业内容**

**对上面数据结构使用你的信息进行填充，studentID是 8 位学号；name 是姓名首字母；score：60-100 数字，填充完使用 echo 命令得到“你的八位学号.der”文件，给出编码过程和echo命令具体内容（5 分）**

- 数据结构

```
studentID 20221414 INTEGER
name xlm IA5String
score 100 INTEGER
```

- 对studentID进行der编码

```
20221414 16进制为1348DE6

T:为0x02

V:0x01 0x34 0x8d 0xe6
```

```
L:0x04

综上，der编码为 02 04 01 34 8d e6
```

- 验证如下：

```
root@Youer:~/shiyan/test1210/dsn# echo -ne "\x02\x04\x01\x34\x8d\xe6" > stuid.der
root@Youer:~/shiyan/test1210/dsn# openssl asn1parse -in stuid.der -inform der
    0:d=0  hl=2 l=   4 prim: INTEGER           :01348DE6
```

- 对name进行der编码

```
T:0x16

L:0x03

V:0x58 0x4C 0x4D

der编码为 16 03 58 4C 4D
```

- 验证如下：

```
root@Youer:~/shiyan/test1210/dsn# echo -ne "\x16\x03\x58\x4C\x4D" > name.der
root@Youer:~/shiyan/test1210/dsn# openssl asn1parse -in name.der -inform der
    0:d=0  hl=2 l=   3 prim: IA5STRING         :XLM
```

- 对score进行der编码

```
99 16进制为63

T:为0x02

V:0x63

L:0x01

der编码为 02 01 63
```

- 验证如下：

```
root@Youer:~/shiyan/test1210/dsn# echo -ne "\x02\x01\x63" > score.der
root@Youer:~/shiyan/test1210/dsn# openssl asn1parse -in score.der -inform der
    0:d=0  hl=2 l=   1 prim: INTEGER           :63
```

- 合并结果：30 0e 02 04 01 34 8d e6 16 03 58 4C 4D 02 01 63

  stuid长度为6、name长度为5、score长度为3，长度共为14，16进制为e

  T：0x30

  L：0x0e

  V：上面连接起来

  综上，der编码为30 0e 02 04 01 34 8d e6 16 03 58 4C 4D 02 01 63

- 使用 echo 命令得到“你的八位学号.der”文件

```
echo -ne "\x30\x0e\x02\x04\x01\x34\x8d\xe6\x16\x03\x58\x4c\x4d\x02\x01\x63" >
20221414.der
```

**使用 od 命令查看“你的八位学号.der”文件的内容，提交运行结果（2分）**

```
root@Youer:~/shiyan/test1210/dsn# od -tx1 20221414.der
0000000 30 0e 02 04 01 34 8d e6 16 03 58 4c 4d 02 01 63
0000020
```

**使用 OpenSSL asn1parse 命令解析“你的八位学号.der”文件，提交运行结果（2分）**

```
root@Youer:~/shiyan/test1210/dsn# openssl asn1parse -in 20221414.der -inform der
    0:d=0  hl=2 l=  14 cons: SEQUENCE
    2:d=1  hl=2 l=   4 prim: INTEGER           :01348DE6
    8:d=1  hl=2 l=   3 prim: IA5STRING         :XLM
   13:d=1  hl=2 l=   1 prim: INTEGER           :63
```