[toc]

课上测试

ch03

作业题目：DER编码基础

完成下面任务（9分）

1. 对 BitString “101101101101”进行 DER编码，提交详细过程和结果。
2. 使用 echo 命令生成 bs.der文件，并使用 OpenSSL asn1parse命令解析，提交命令和结果（4 分）
3. 对 基于SM2算法和SHA256算法的签名的OID 1.2.156.197.1.503进行 DER 编码，提交详细过程和结果，并使用 OpenSSL asn1parse命令解析，提交命令和结果。（5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”

实际过程

1. 对 BitString “101101101101”进行 DER编码，提交详细过程和结果。
    - 类型：0x03
    - 填充：
        - 填充判断：“10 11 01 10 11 01”共计12位，不是8的倍数，需要补4个0在末尾
        - 所以“值”字段的前导字节设置为“0x04”
        - 填充后的结果“10 11 01 10 11 01 00 00”，其十六进制表示为“B6 D0”
    - 值的字节数（算上前导字节）是3，小于128，所以长度用“03”表示
    - 综上，编码结果是： 03 03 04 B6 D0 2.使用 echo 命令生成 bs.der文件，并使用 OpenSSL asn1parse命令解析，提交命令和结果

```
root@Youer:~/TestInClass/ClassTest/testSM3Pad# echo -n -e
'\x03\x03\x04\xB6\xD0' > bs.der
root@Youer:~/TestInClass/ClassTest/testSM3Pad# openssl asn1parse -in bs.der
-inform DER
    0:d=0  hl=2 l=   3 prim: BIT STRING
```

3.对基于SM2算法和SHA256算法的签名的OID 1.2.156.197.1.503进行 DER 编码，提交详细过程和结果，并使用 OpenSSL asn1parse命令解析，提交命令和结果。（5分）

- 编码过程
    - 类型：06
    - 前两个数字：40*1 + 2= 42 >> 0x2A

    - 后面的数字：81 1C 81 45 01 83 77
        - 156对应 0x81 0x1C
        - 197对应 0x81 0x45
        - 1对应 01
        - 503对应 0x83 0x77
    - 综上，长度是 08
    - 最终编码是： 06 08 2A 81 1C 81 45 01 83 77
- 使用 OpenSSL asn1parse命令解析

```
root@Youer:~/TestInClass/ClassTest/testSM3Pad# echo "06082A811C8145018377" |
xxd -r -p | openssl asn1parse -inform der
    0:d=0  hl=2 l=   8 prim: OBJECT            :1.2.156.197.1.503
```

- 同时可以在线解码