[toc]

课上测试

ch03

作业题目：DER编码分解（GMT0009）

完成下面任务（9分）

1. 在 Ubuntu 或 openEuler 中完成任务（推荐openEuler）
2. 使用 GmSSL 命令对“你的8 位学号+姓名的首字母”进行数字签名，并参考附件 GMT0009 分解得到签名值，提交签名值结果。（4 分）
3. 使用 GmSSL 命令对“你的8 位学号+姓名的首字母”进行加密 ，并参考附件 GMT0009 分解得到密文数据，提交密文值。（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”

- github链接

作业过程

使用命令的部分

- 使用GmSSL命令对8位学号+姓名的首字母进行数字签名

```
root@Youer:~/shiyan/test1210/newsm2# gmssl sm2keygen -pass 1234 -out sm2.pem -
pubout sm2pub.pem
root@Youer:~/shiyan/test1210/newsm2# echo -n "20221414xlm" | gmssl sm2sign -key
sm2.pem -pass 1234 -out sm2.sig -id 1234567812345678
root@Youer:~/shiyan/test1210/newsm2# xxd sm2.sig
00000000: 3046 0221 00d1 c838 374f 88ca cdc1 c2dd  0F.!...87O......
00000010: 9936 1d59 0adf 2b9a 7f37 9fe4 6e36 77f9  .6.Y..+..7..n6w.
00000020: de49 a9d6 3402 2100 aecb b004 e1f0 4ca5  .I..4.!.......L.
00000030: a6e5 e54a d713 273c 35a2 1a92 15ae 50e9  ...J..'<5.....P.
00000040: a917 16a0 5c0f f443                      ....\..C
```

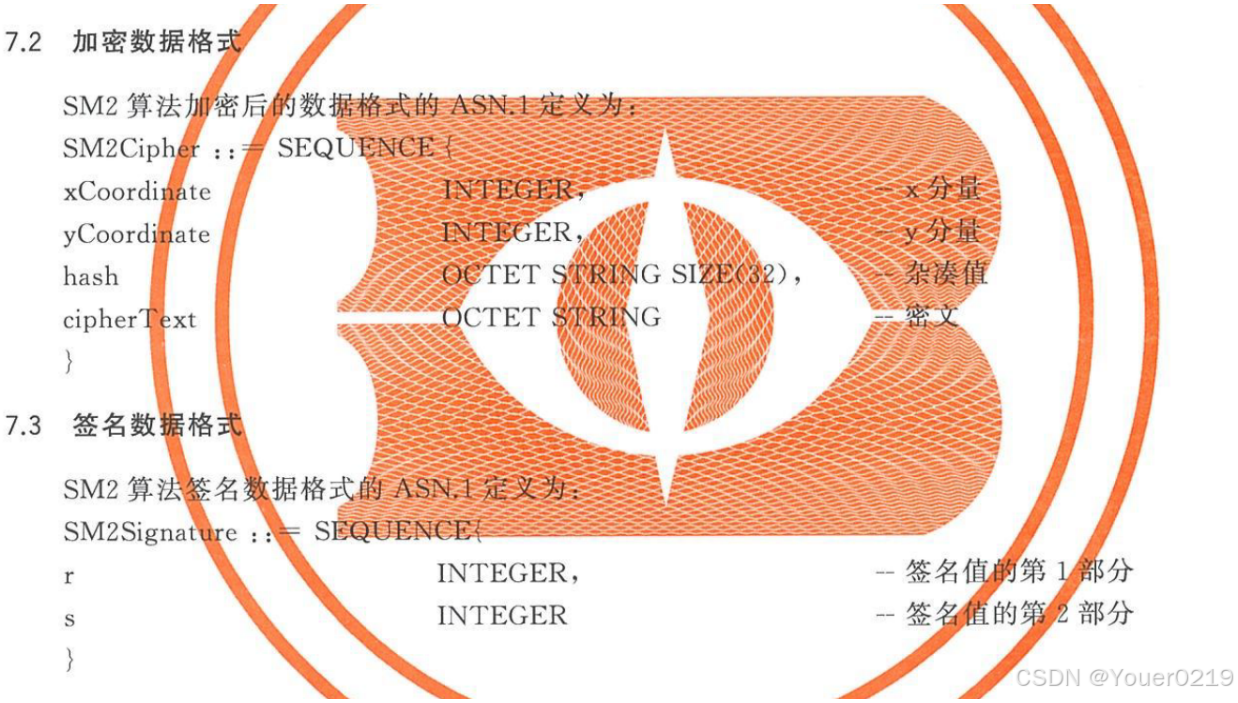
- 使用GmSSL命令对8位学号+姓名的首字母进行加密

```
root@Youer:~/shiyan/test1210/newsm2# echo -n "20221414xlm" | gmssl sm2encrypt -
pubkey sm2pub.pem -out sm2.der
```

```
root@Youer:~/shiyan/test1210/newsm2# xxd sm2.der
00000000: 3075 0221 0099 b5f1 7f41 2033 2ab6 a147  0u.!.....A 3*..G
00000010: 95d9 cd99 894f a9e0 9dc3 4faa 15f3 bf68  .....O....O....h
00000020: 66f3 4c6b a702 2100 8d43 c41e 4111 9dd9  f.Lk..!..C..A...
00000030: 4bcb 3a71 b7b5 7e43 8ed7 c604 c34f bd39  K.:q..~C.....O.9
00000040: 2ab4 ba82 19ea dbd4 0420 5e05 9111 5cd3  *........ ^...\.
00000050: d23d e5e3 13b1 e83b b0b6 00e4 3282 375c  .=.....;....2.7\
00000060: 0958 402a a494 4108 0c35 040b 82d3 b974  .X@*..A..5.....t
00000070: acb2 0214 8048 35                        .....H5
```

分解签名和加密结果

- 标准内容：



7.2 加密数据格式

SM2 算法加密后的数据格式的 ASN.1 定义为：

```
SM2Cipher ::= SEQUENCE {
xCoordinate     INTEGER,              -- x 分量
yCoordinate     INTEGER,              -- y 分量
hash            OCTET STRING SIZE(32), -- 杂凑值
cipherText      OCTET STRING          -- 密文
}
```

7.3 签名数据格式

SM2 算法签名数据格式的 ASN.1 定义为：

```
SM2Signature ::= SEQUENCE{
r               INTEGER,              -- 签名值的第 1 部分
s               INTEGER               -- 签名值的第 2 部分
}
```


参考附件 GMT0009 分解得到签名值,提交签名值结果

- 原始签名值：

```
00000000: 3046 0221 00d1 c838 374f 88ca cdc1 c2dd
00000010: 9936 1d59 0adf 2b9a 7f37 9fe4 6e36 77f9
00000020: de49 a9d6 3402 2100 aecb b004 e1f0 4ca5
00000030: a6e5 e54a d713 273c 35a2 1a92 15ae 50e9
00000040: a917 16a0 5c0f f443
```

- 解码后的数据：

```
<SEQUENCE>
<INTEGER>0x00D1C838374F88CACDC1C2DD99361D590ADF2B9A7F379FE46E3677F9DE49A9D63
4</INTEGER>
<INTEGER>0x00AECBB004E1F04CA5A6E5E54AD713273C35A21A9215AE50E9A91716A05C0FF44
```

```
3</INTEGER>
</SEQUENCE>
```

- 实际签名值：参考标准，实际签名值为r和s
  - r：0x00D1C838374F88CACDC1C2DD99361D590ADF2B9A7F379FE46E3677F9DE49A9D634
  - s: 0x00AECBB004E1F04CA5A6E5E54AD713273C35A21A9215AE50E9A91716A05C0FF443

参考附件 GMT0009 分解得到密文数据，提交密文值

- 原始加密值

```
00000000: 3075 0221 0099 b5f1 7f41 2033 2ab6 a147
00000010: 95d9 cd99 894f a9e0 9dc3 4faa 15f3 bf68
00000020: 66f3 4c6b a702 2100 8d43 c41e 4111 9dd9
00000030: 4bcb 3a71 b7b5 7e43 8ed7 c604 c34f bd39
00000040: 2ab4 ba82 19ea dbd4 0420 5e05 9111 5cd3
00000050: d23d e5e3 13b1 e83b b0b6 00e4 3282 375c
00000060: 0958 402a a494 4108 0c35 040b 82d3 b974
00000070: acb2 0214 8048 35
```

- 解码后的数据

```
<SEQUENCE>
<INTEGER>0x0099B5F17F4120332AB6A14795D9CD99894FA9E09DC34FAA15F3BF6866F34C6BA
7</INTEGER>
<INTEGER>0x008D43C41E41119DD94BCB3A71B7B57E438ED7C604C34FBD392AB4BA8219EADBD
4</INTEGER>
<OCTET_STRING>0x5E0591115CD3D23DE5E313B1E83BB0B600E43282375C0958402AA4944108
0C35</OCTET_STRING>
<OCTET_STRING>0x82D3B974ACB20214804835</OCTET_STRING>
</SEQUENCE>
```

- 参考标准，加密值由以下部分组成：
  - xCoordinate：椭圆曲线点的x坐标。
  - yCoordinate：椭圆曲线点的y坐标。
  - hash：消息的哈希值。
  - cipherText：加密后的密文
- 实际密文数据：0x82D3B974ACB20214804835