[toc]

课上测试

ch03

作业题目：

完成下面任务（10分）

1. 使用 OpenSSL 生成长度为70字节的随机数，最后添加“你的8位学号+姓名首字母”的 ASCII 码，得到HEX 字符串S1，提交S1。（4 分）
2. 按照商用密码标准对 S1进行填充，提交填充过程和填充好的HEX 字符串S2。要包含详细填充过程。（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.s1:596b117c1b8cc1d358028ca76e5fb84a622496cd606e9ed6aad5e5f6ab4c39ff491ff2ecad9382d0120eeedeb457add1524bc5ac37055564cbdb2233cdaf50ba6e7ff0ca8990 + 32 30 32 32 31 34 31 34 78 6c 6d
`root@Youer:~/TestInClass/ClassTest/testSM3Pad# openssl rand -hex 70 596b117c1b8cc1d358028ca76e5fb84a622496cd606e9ed6aad5e5f6ab4c39ff491ff2ecad9382d0120eeedeb457add1524bc5ac37055564cbdb2233cdaf50ba6e7ff0ca8990`

2.按照商用密码标准对 S1进行填充:

2.1.计算1000000中0的个数： 512+448-（81*8）= 312位,39字节，所以0的个数是311个 2.2.末尾添加“1”，补0致448位：
596b117c1b8cc1d358028ca76e5fb84a622496cd606e9ed6aad5e5f6ab4c39ff491ff2ecad9382d0120eeedeb457add1524bc5ac37055564cbdb2233cdaf50ba6e7ff0ca89903230323231343134786c6d + 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2.3.长度为81字节，最后部分就为64比特的000...... 1010001,也就是十六进制的 00 00 00 51 2.4.综合来看，s2为：
596b117c1b8cc1d358028ca76e5fb84a622496cd606e9ed6aad5e5f6ab4c39ff491ff2ecad9382d0120eeedeb457add1524bc5ac37055564cbdb2233cdaf50ba6e7ff0ca89903230323231343134786c6d + 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 + 00 00 00 51
也就是：
596b117c1b8cc1d358028ca76e5fb84a622496cd606e9ed6aad5e5f6ab4c39ff491ff2ecad9382d0120eeedeb457add1524bc5ac37055564cbdb2233cdaf50ba6e7ff0ca89903230323231343134786c6d80000000000000000000000000000000000000000000000000000000000000000000000000000051