**Implement sm2 with RFC6979**

**网安2020级 徐徽成 202000460143**

注：实验在python环境下运行

准备事项

sm2 python代码[[1]](#footnote-0)

这里采用简单的调用gmssl库实现sm2加密



**RFC6979原理：[[2]](#footnote-1)**

重新定义私钥k = SHA256(d + HASH(m))

其中d为原私钥

则添加下图步骤完成新私钥的生成



运行结果：



1. https://blog.csdn.net/u014651560/article/details/113744296 [↑](#footnote-ref-0)
2. https://www.8btc.com/article/38766 [↑](#footnote-ref-1)