impl sm2 with RFC6979

项目代码说明

由于ECDSA方案因代码实现时随机源质量不高屡次出现问题，RFC6979文档定义了确定性数字签名生成过程。本实验我依据该文档，实现了sm2中的随机数k生成算法。

- sm2.py 该代码**引用自** gmssl包https://github.com/duanhongyi/gmssl，在源代码上稍作修改调整
- gen_k.py 依照RFC6979文档独立完成，实现随机数k生成算法
- test.py 测试代码

运行指导

将三个py文件下载到同一目录下，运行test.py文件进行测试

代码运行截图

```
In [1]: runfile('E:/实验报告/创新课/project4/test.py', wdir='E:/
实验报告/创新课/project4')
message:b'111'
signature:
331db8d1a44437153dbc644d8aba99732d214b752be2cf7abe9ca7715a44f30
0d4cdcf195de810b1a16fd055ce27f66b724804ed680c08687063ad64404491
47
verify:True

In [2]: runfile('E:/实验报告/创新课/project4/test.py', wdir='E:/
实验报告/创新课/project4')
message:b'111'
signature:
331db8d1a44437153dbc644d8aba99732d214b752be2cf7abe9ca7715a44f30
0d4cdcf195de810b1a16fd055ce27f66b724804ed680c08687063ad64404491
47
verify:True

In [3]:
```

测试对消息“111”签名并验签通过，算法为确定性算法，两次运行结果相同。

贡献说明

张雨欣一人完成，其中sm2.py引用自gmssl包