

源程序清单

1.Math.py

一些常见的数学运算、编码运算，包含欧几里得算法、扩展的欧几里得算法、整数求模逆算法、快速模幂算法、米勒拉宾素性检验算法、大素数生成算法、字节串转整数算法、整数转字节串算法、十六进制串转二进制串算法、二进制串转十六进制串算法、字节串转二进制串算法、二进制串转字节串算法。

2.Block_Cipher_SM4.py

SM4分组密码，包含CTR和OFB两种工作模式。

3.Public_Key_SM2.py

SM2公钥加密算法。

4.DS_ElGamal.py

ElGamal数字签名算法。

5.Hash_SM3

SM3哈希算法。

6.CLI.py

一个命令行界面设计，实现与用户之间的交互。

7.test.py

测试密码库中包含的所有函数的正确性和可用性。

8.Collections

包含密码库的所有算法模块及测试模块。