

《应用密码学》课程

实践报告



**实践题目 简易安全数据传输系统**

**学生姓名** borgeous

**学 号** xxxxxxx

**实验时间** 6月7日

1. 实践目的

（简要给出本次课程实践的目的）

通过本综合实践，学生将实际应用国密算法，以加深对课程中介绍的对称加密、非对称加密/公钥加密、哈希算法、数字签名等密码学概念的理解。通过构建一个简易的安全数据传输系统，更深刻地理解国密算法在实际数据安全通信中的应用，认识到这些技术在保护信息安全中的重要性，并培养合规的密码技术使用习惯

1. 实践内容

（简要给出课程实践的主要内容及相关原理）

实现对待传输目标数据的认证性、机密性和完整性保护。假设存在甲乙两方需进行数据的安全传输，甲方自选5M大小的数据作为目标数据，本地产生随机数作为文件的加/解密密钥，该密钥可用于对称加密方案对数据实施机密性保护；此外，甲方需对目标数据的散列值计算数字签名，以便乙方确认数据的来源以及是否被篡改。同时，为确保乙方能够正确的恢复出数据，甲方需用乙方的公钥对密钥进行加密传输。请以甲方的身份实现上述功能，并为乙方提供验证程序，验证程序能够恢复用于对文件进行解密的密钥，然后实现解密，并验证甲方签名是否正确，以及数据是否被正确恢复。

1. 实践环境

（简要给出完成课程实践的软硬件实验环境）

操作系统：win11

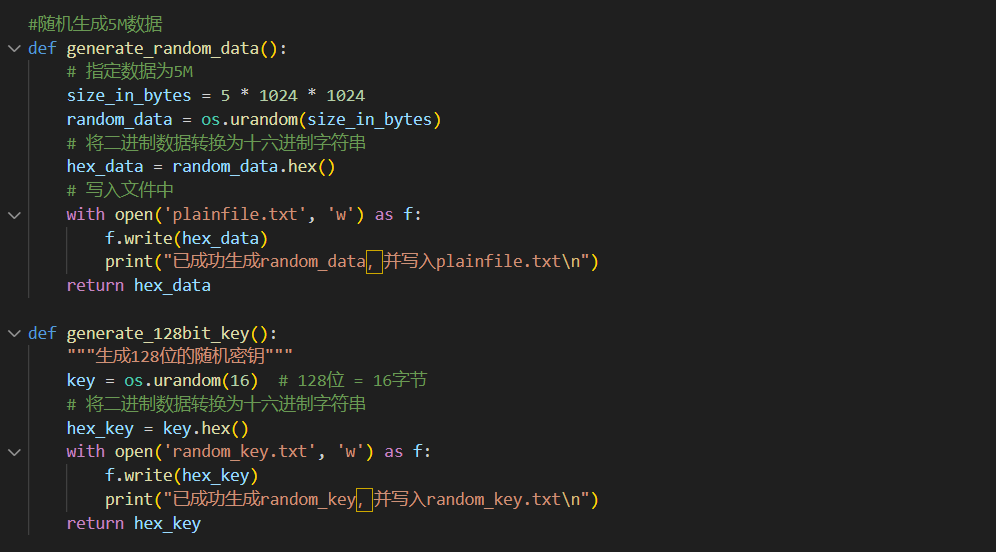
IDE：VScode

CPU：AMD锐龙系列

1. 实践过程与步骤

（以图文方式给出课程实践过程、关键步骤和相关结果）

首先我们随机生成5M数据和随机密钥key，以及生成甲乙的公私钥，并写到相关的文件中

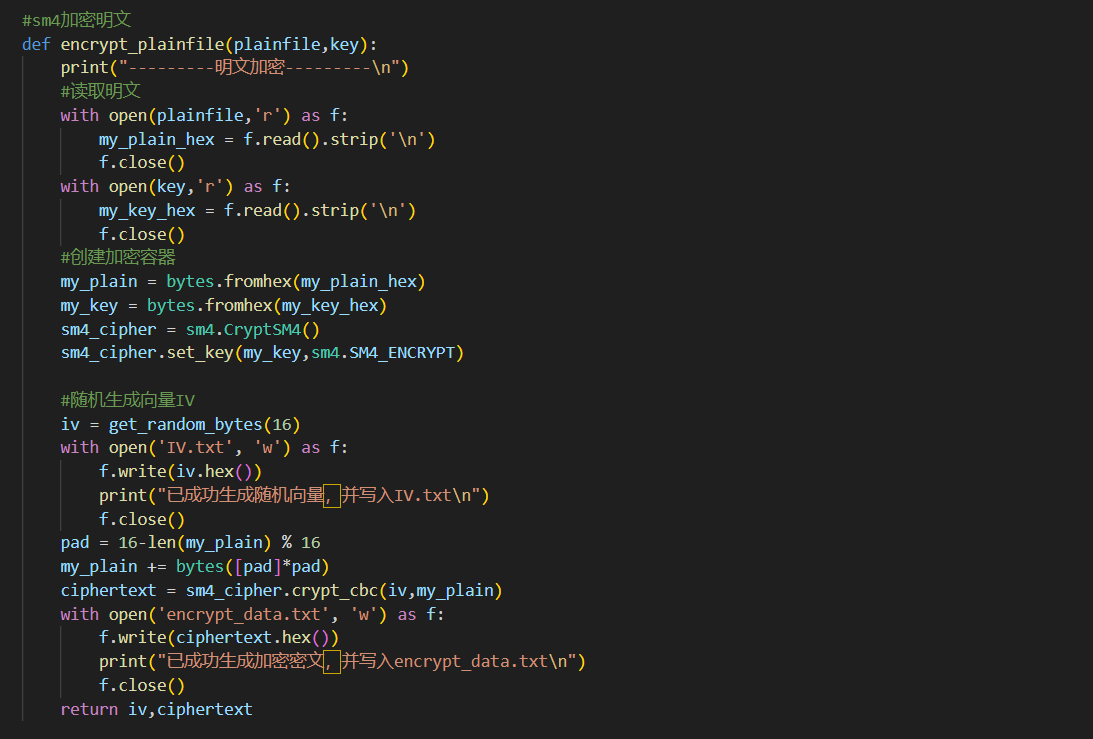




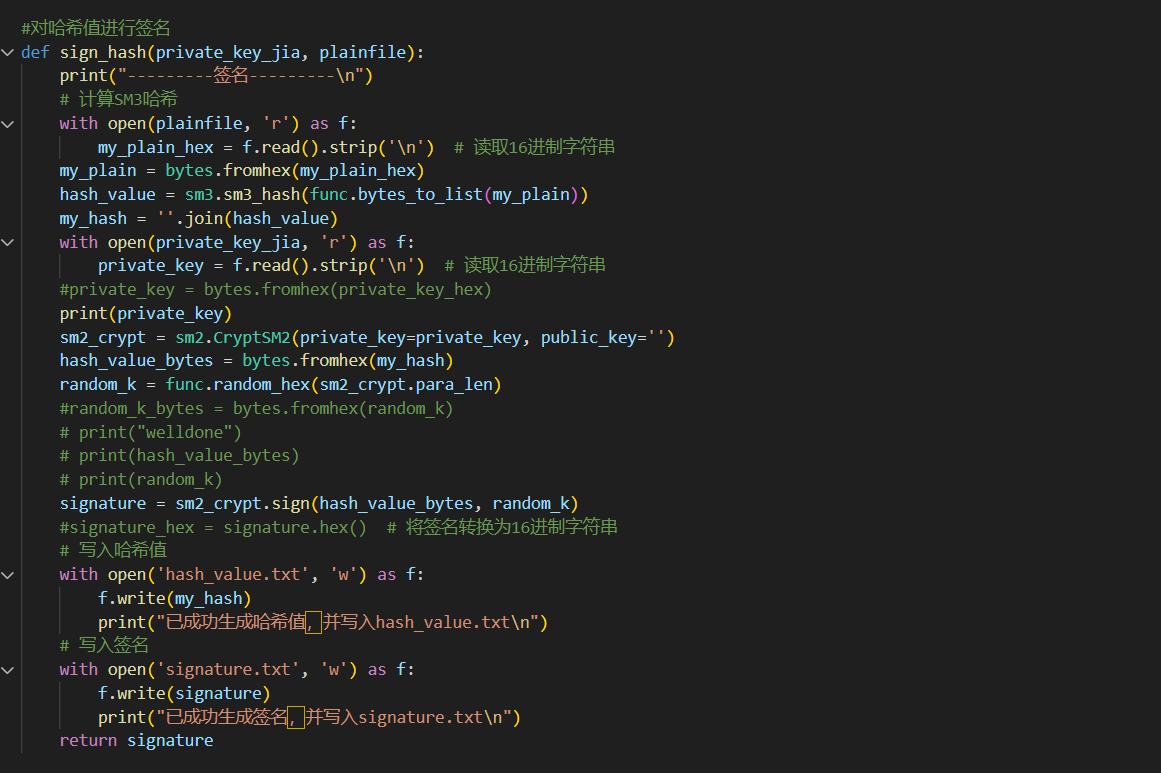
紧接着，我们用乙的公钥对随机密钥key进行加密



接着使用sm4算法对生成的明文进行加密

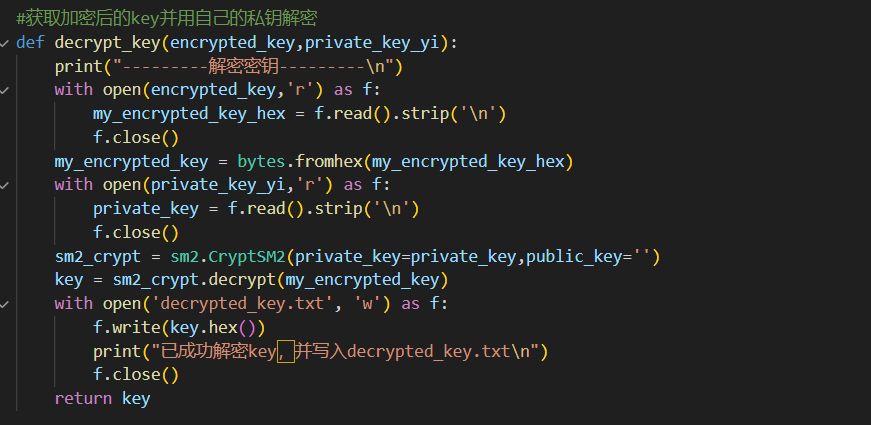


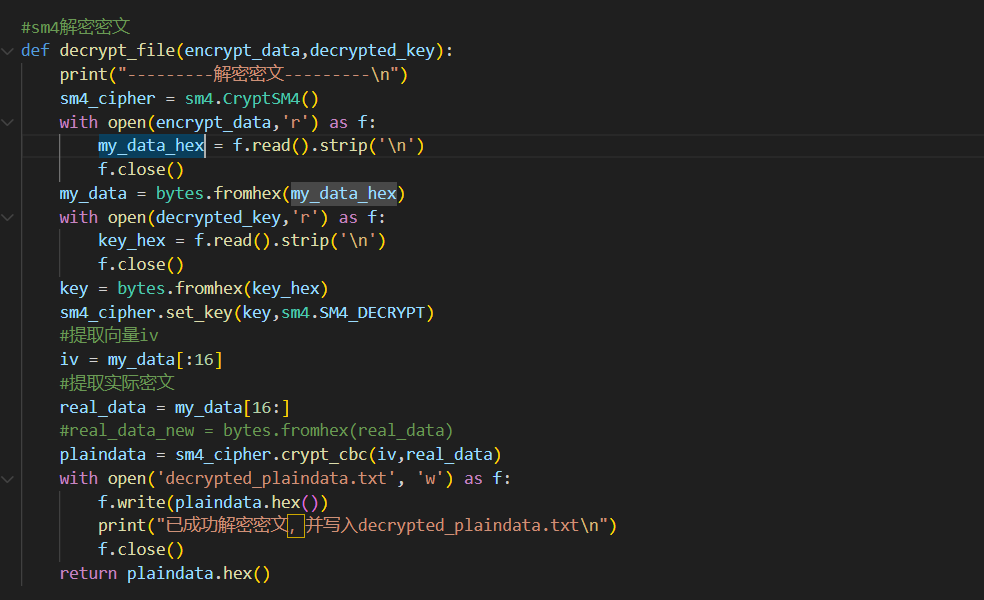
之后对原文件计算其哈希，并对哈希值进行签名



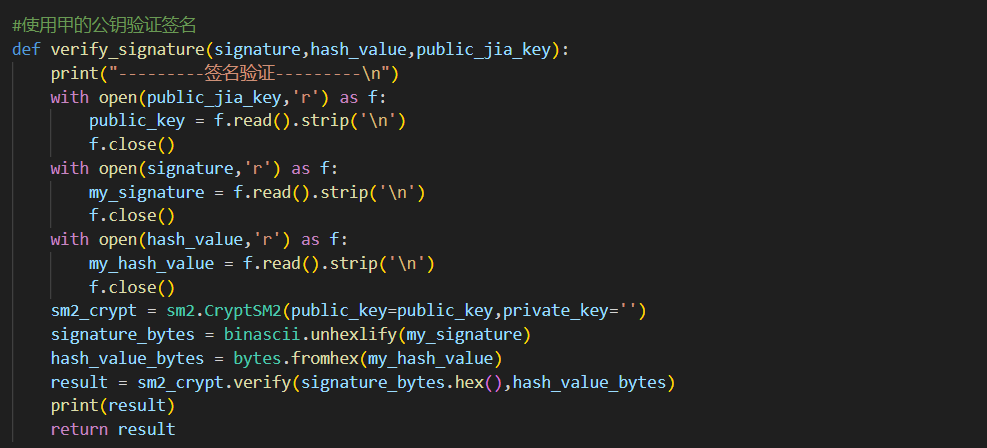
之后设计乙方的解密和验证工作

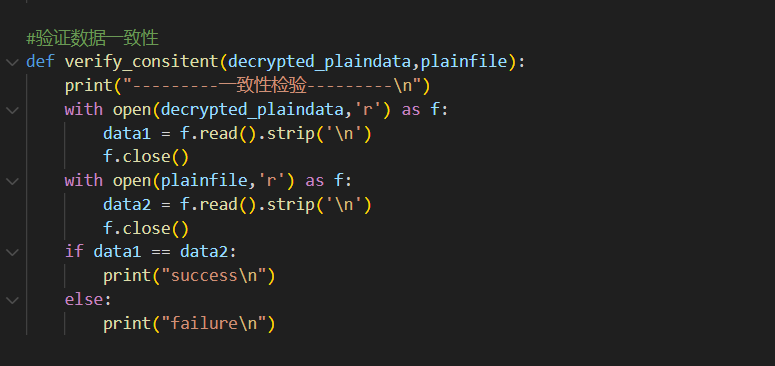
首先拿自己的私钥并对加密后的key进行解密，之后再用sm4进行密文解密



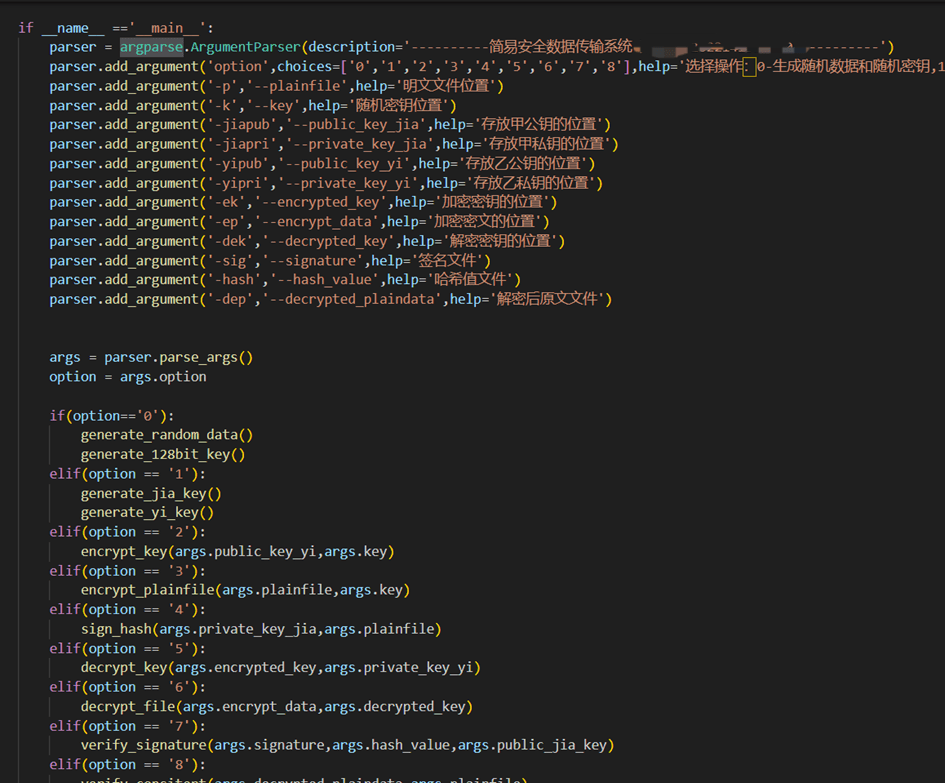


之后使用甲的公钥进行签名验证，以及对比原文和解密后的密文，看是否符合一致性检验





最后完成主函数的设计，依旧使用argparse库



1. 程序设计方案

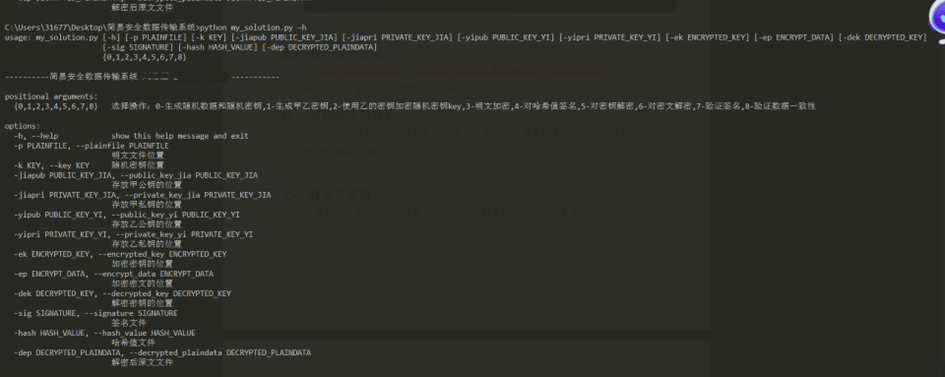
（对程序设计课程实践，给出程序流程图、数据结构及I/O接口描述）

相关文件见github或者源代码压缩包

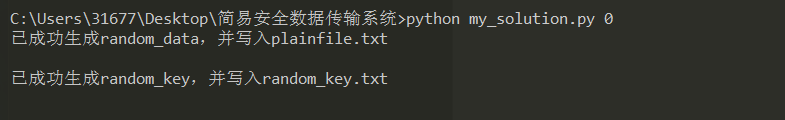
1. 实践结果与分析

（给出实践结果，验证或判断其正确与合理性，完成实践要求的分析与思考）

-h进入帮助页面

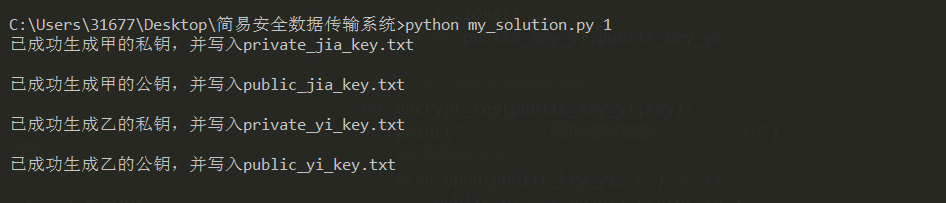


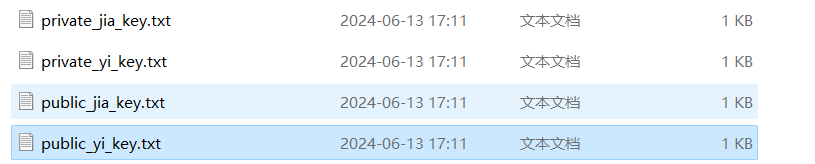
选择操作0，进行随机数据的生成和随机密钥的生成



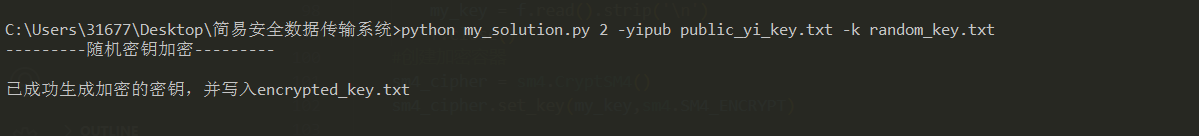


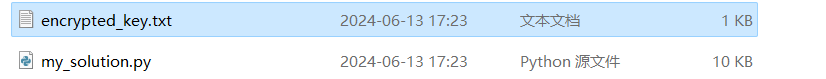
紧接着，我们进行操作1，生成甲和乙的公钥和私钥



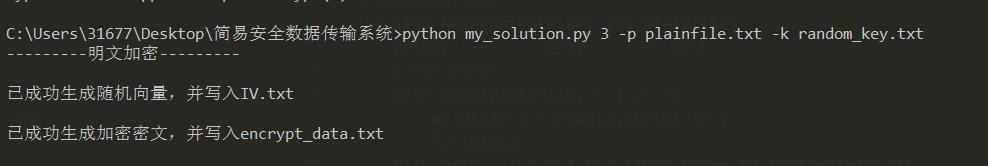


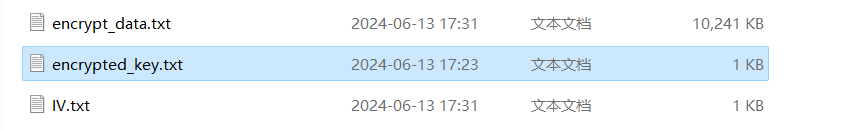
下一步我们用乙的公钥对随机密钥进行加密



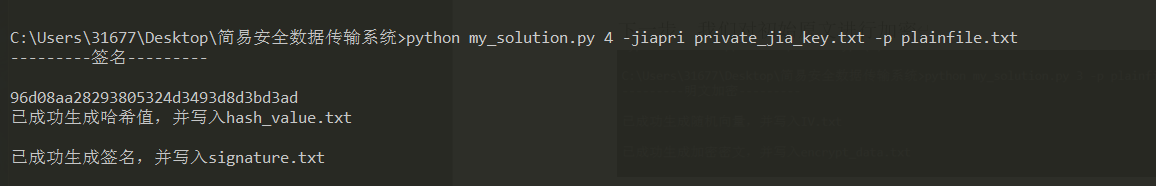


下一步，我们对初始原文进行加密



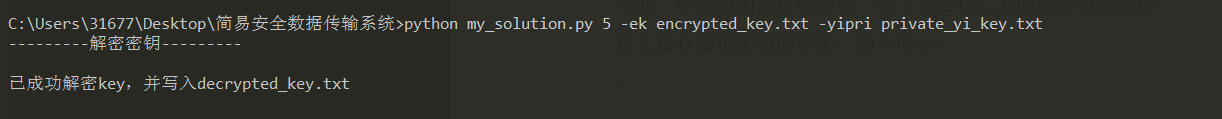


接着，我们进行哈希值的签名

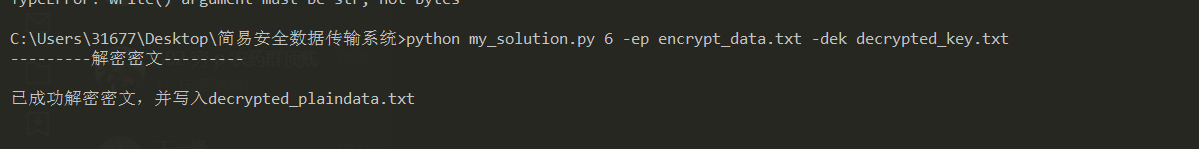


至此，甲方的加密过程结束，接下来进行乙方的解密验证过程

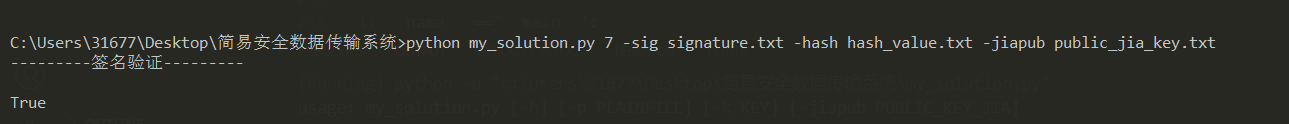
首先进行随机密钥的解密，如下所示



之后拿解密出来的key进行密文的解密

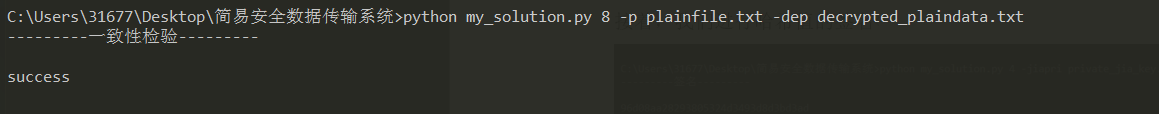


接下来使用甲的公钥进行签名的验证



如图所示，签名验证成功

接下来进行最后一步，进行数据一致性的检验



检验成功，实验至此结束

1. 体会与收获

（简要给出本次实践的体会与收获，以及对课程实践有关意见和建议）

通过对sm国密算法的使用，我更清楚的了解了国密算法是如何调用的，以及对数据是byte形式还是16进制有了很深刻的了解，同时对加密使用公钥，签名使用私钥，以及进行签名验证的全流程有了很清楚的了解，在做实验的过程中，自己的代码能力得到进一步提升

评阅人： 日期