

《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** XX

**学 号** XXXXXXXXXXX

**实验时间** XX月XX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）

1. 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。
2. 参数及算法要求：文件的加解密密钥长度为128bit，对称加密的算法为**SM4（CBC模式）**，甲方的数字签名为**SM2签名**（**哈希算法为SM3**）。
3. 要求提供明文文件、密钥文件、数据密文文件、密钥密文文件、以及甲方的数字签名，验证程序能够分别实现以下功能：
   1. 获取文件加解密密钥：以命令行形式指定密钥密文文件和乙方的公钥，完成对密钥文件的解密，输出密钥并将密钥本地保存为恢复密钥文件；
   2. 对文件进行解密：以命令行形式指定数据密文文件和恢复密钥文件，完成对数据的解密，输出恢复的明文文件，将恢复的文件保存为恢复明文文件；
   3. 验证签名：以命令行形式指定甲方数字签名、恢复的明文文件，完成对甲方数字签名正确与否的验证，输出结果为true或false；
   4. 完成数据一致性的检查：以命令行形式指定明文文件和恢复明文文件，如果两文件一致，则输出success，否则输出failure.
4. 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：windows 11

Cpu：AMD Ryzen 7 5800H with Radeon Graphics 3.20 GHz

编译器：pthon-3.10

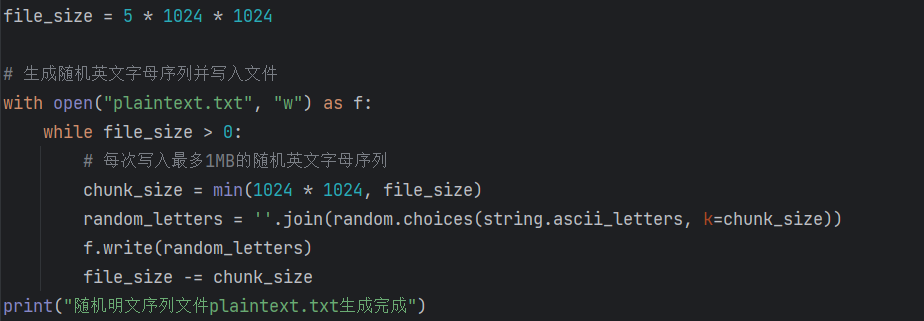
内存：16GB

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）

首先写一个initialize.py文件用于初始化

生成随机5m大小文件



随机生成公钥私钥



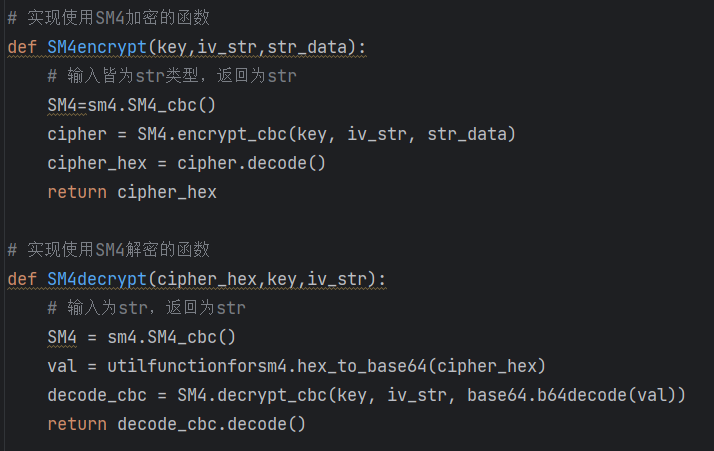
随即生成密钥



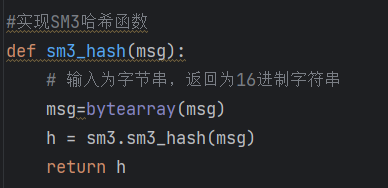
随机生成iv



SM4加解密函数



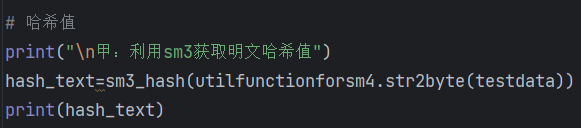
SM3哈希函数



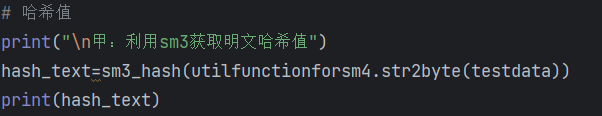
然后从文件中读取到所需的内容



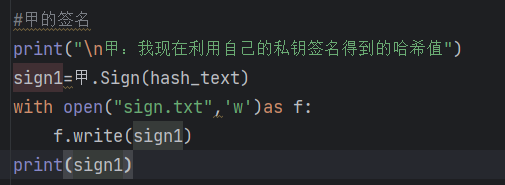
之后进行对称加密并将密文写入文件中



然后获取明文的哈希值



甲对哈希值进行签名并将签名写入文件中



甲利用乙的公钥加密对称密钥并写入文件中



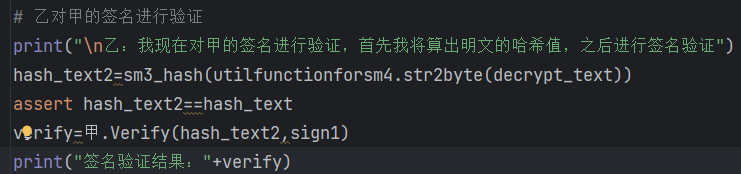
乙恢复加密的密钥



乙利用加密密钥恢复明文



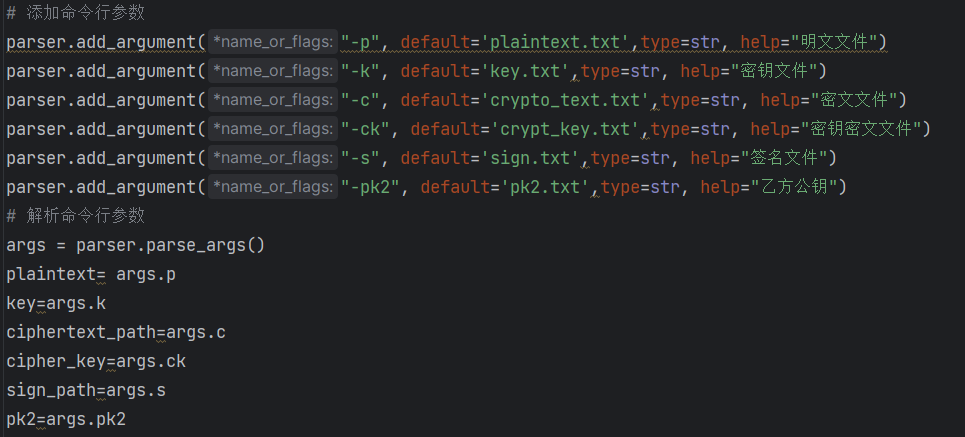
乙对甲的签名进行验证



输出结果



之后利用main.py文件实现命令行功能



功能a



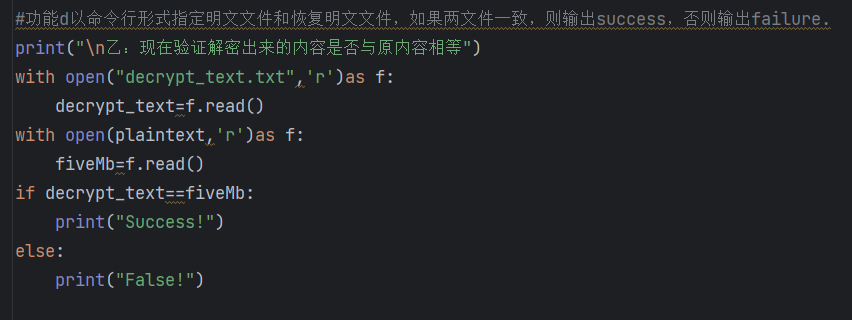
功能b



功能c



功能d



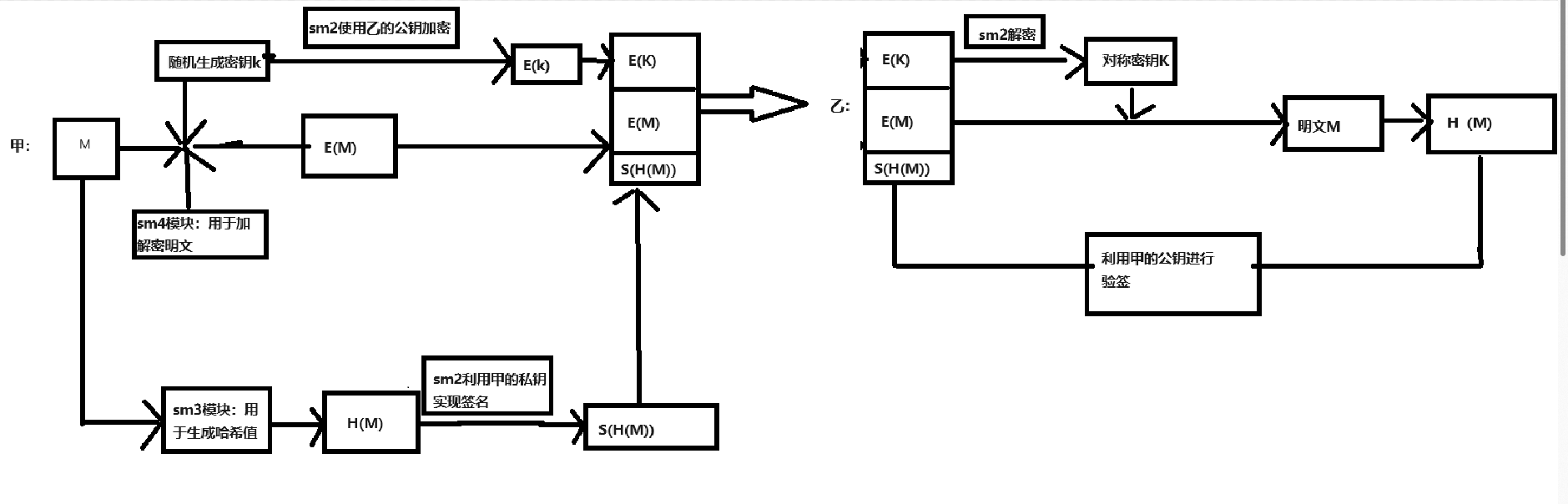
输出：



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）

本项目基于gmssl库实现，实现了sm2加解密，数字签名的功能，sm3哈希函数以及sm4加解密的功能，分别对应sm2.py,sm3.py,sm4.py。以下是实验流程是设计图



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）

初始化（同时也是要求的整个过程）结果：



Main函数结果：



由结果可以看出本次实验成功使用了sm2，sm3以及sm4来实现了简易的安全传输系统

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）

通过参与本次《应用密码学》的课程实践，我深刻体会到了密码学在现实世界中的重要性和实用性。在构建简易安全数据传输系统的过程中，我不仅加深了对对称加密、非对称加密、哈希算法和数字签名等密码学基础概念的理解，而且对国密算法的实际应用有了更为直观的认识。

在实验中，我首次将课堂上学到的理论知识应用到实际问题中，这种从理论到实践的转变让我更加深刻地理解了密码学的原理和应用。

通过实现SM4加密、SM3哈希以及SM2签名的具体过程，我对这些算法的内部机制和实现细节有了更深入的了解。

在实验过程中遇到的各种技术难题，如密钥管理、数据一致性验证等，都锻炼了我分析问题和解决问题的能力。

实验结果显示，我成功地使用国密算法构建了一个简易但功能完整的安全数据传输系统。这不仅验证了所学知识的实用性，也增强了我将密码学技术应用于实际问题的信心。

评阅人： 日期