《应用密码学》课程综合实践：简易安全数据传输系统

实践目的：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。

实践要求：

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. 用**Python**语言完成程序。可参考“铜锁”开源库以及‘gmssl’等密码库实现。
5. 最终上交的作业包括：电子版的实践报告和程序源代码，要求由源代码能重新正确生成可执行代码。
6. 实践报告应包括以下内容：作业标题、学号、姓名、E-mail、作业内容描述、实验环境描述、实验过程简述、实验结果（按照对验证程序的要求输出对应功能的运行结果，关键步骤请截图）、作业的收获和体会。实践报告模版与之前发布的模版及要求相同。