《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. 假设甲方自选 5M 大小的数据作为目标数据M，需在确保数据的认证性、机密性和完整性前提下，向乙方进行数据的安全传输。学生需根据各类安全性要求选择使用对应的密码学算法。

2. 各类算法及参数要求：

   1) 对称加密的算法为 **SM4，工作模式为 CBC 模式，128bit/16byte 初始向量** IV 的 16 进制表示为 5072656E7469636548616C6C496E632E，SM4 加解密密钥K为本地产生的满足算法密钥长度要求的随机数，该密钥可用于对称加密方案对数据实施机密性保护$C = SM4(K, M)$；

   2) 签名算法为 **SM2 签名**，其中**哈希运算的算法为 SM3**。签名算法的签名密钥$SK1$和验证密钥$PK1$由签名方（甲方）根据选取的开源库，调用对应算法的密钥生成算法产生，并根据实际使用需要，将验证密钥发送给验证方（乙方）以完成签名验证。签名方（甲方）需对目标数据的散列值$H(M)$计算数字签名$Sig_{SK1}(H(M))$，以便验证方（乙方）确认数据的来源以及是否被篡改。

   3) 为确保接收方（乙方）能够正确的恢复出数据，甲方需将用于加密目标数据M的 SM4 加解密密钥K安全的传输给接收方（乙方）。故需使用公钥加密算法。**公钥加密算法为 SM2 公钥加密算法**，公钥加密算法的加密密钥$PK2$和解密密钥$SK2$由接收方（乙方）根据选取的开源库，调用对应算法的密钥生成算法产生，并将公钥发送给需要对密钥K进行保护的另一方（甲方），以完成对密钥的加密。

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，并分别以甲方和乙方的身份提供对应功能的程序以及可供对方使用的验证程序。相关程序能够分别实现以下功能：

   a 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；

   b 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；

   c 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；

   d 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.

   e 提供本地产生的密钥文件的保护措施.

4. 可用熟悉的编程语言如 **Python、C、C++等**语言完成程序。可参考“铜锁”开源库、‘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。