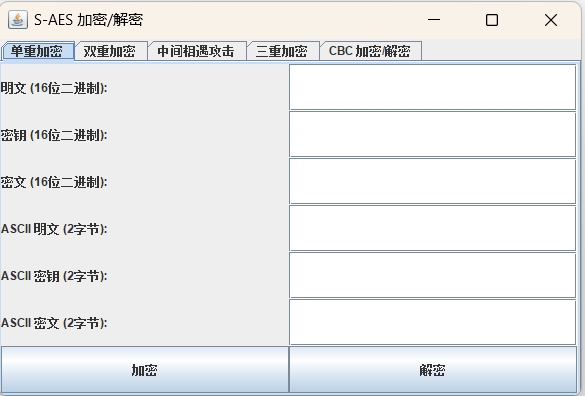
**第1关：基本测试**

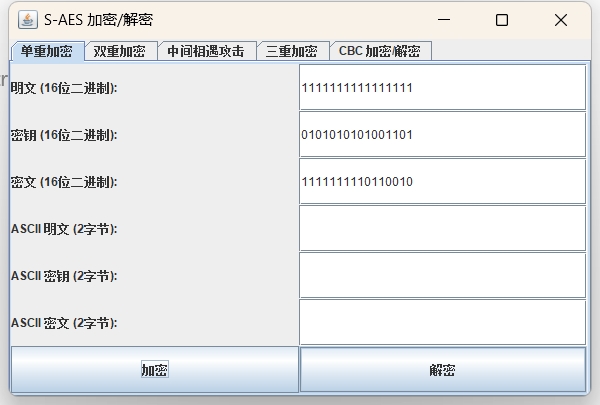
根据S-AES算法编写和调试程序，提供GUI解密支持用户交互。输入可以是16bit的数据和16bit的密钥，输出是16bit的密文。

Gui界面：



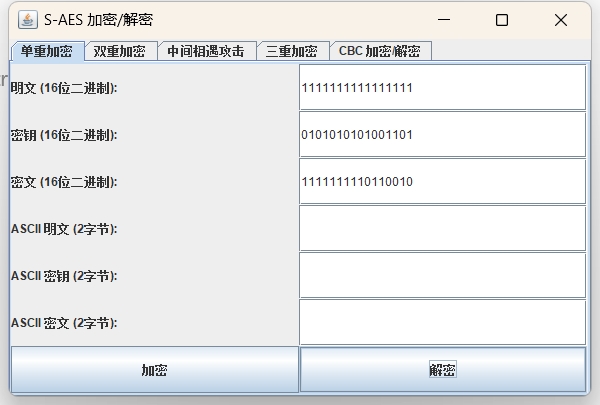
（加密）输入16bit的明文和密钥，输出为16位的密文：



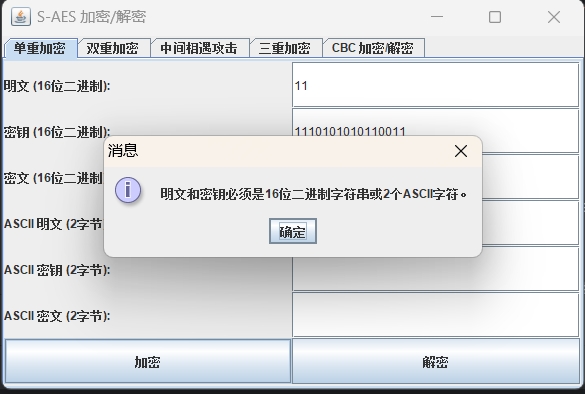


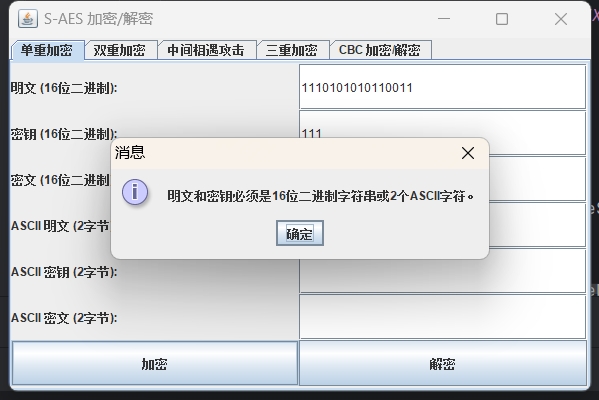
（解密）输入16bit的密钥和明文，输出为16位的明文：





如果明文和密钥输入不是16bit，会出现如下提示：

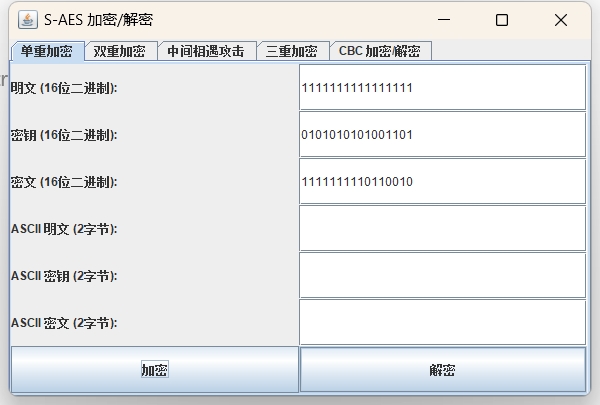




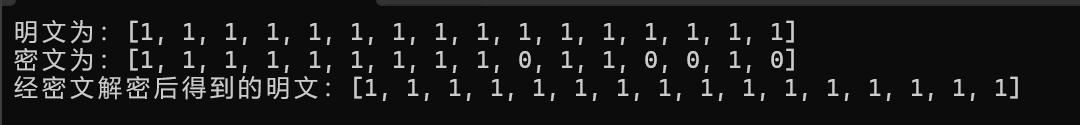
**第2关：交叉测试**

考虑到是"算法标准"，所有人在编写程序的时候需要使用相同算法流程和转换单元(替换盒、列混淆矩阵等)，以保证算法和程序在异构的系统或平台上都可以正常运行。经过测试，得出结果相同：

我们组：



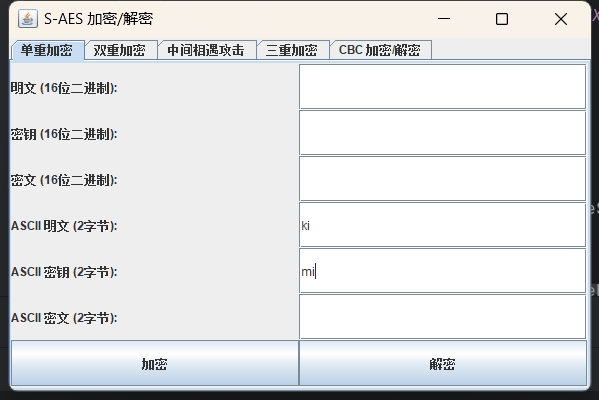
许诺组（人民当家作组）：

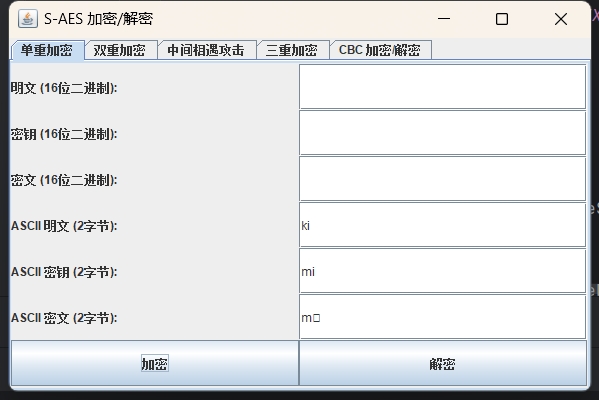


**第3关：扩展功能**

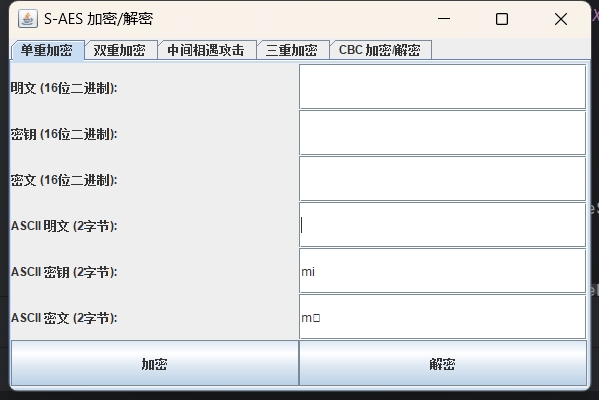
考虑到向实用性扩展，加密算法的数据输入可以是ASII编码字符串(分组为2 Bytes)，对应地输出也可以是ACII字符串(很可能是乱码)。

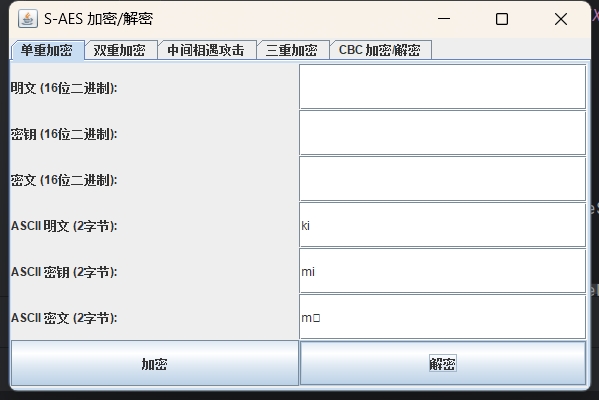
加密：



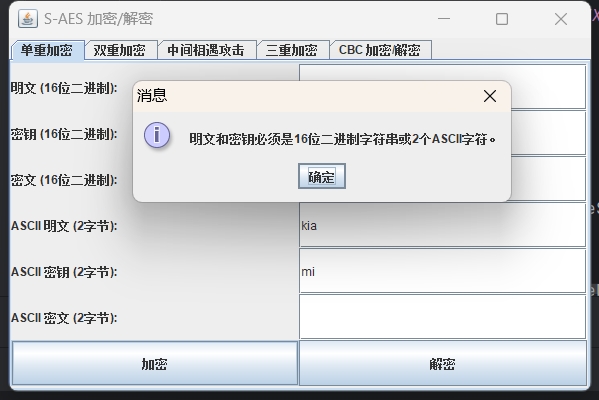


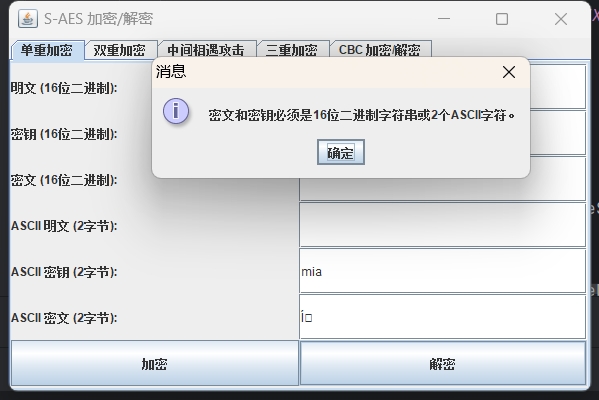
解密：





如果明文和密钥输入不是2bit，会出现如下提示：



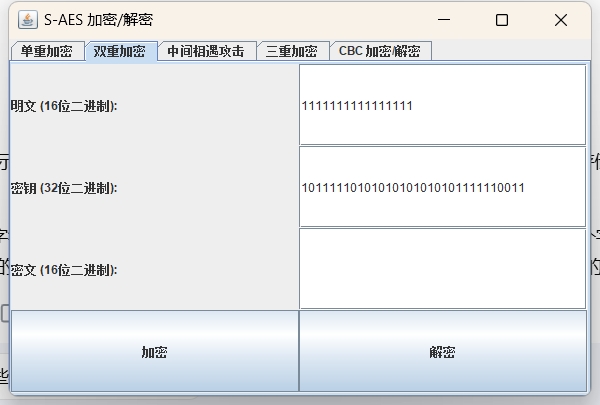


**第4关：多重加密**

4.1 双重加密

将S-AES算法通过双重加密进行扩展，分组长度仍然是16 bits，但密钥长度为32 bits。

加密：





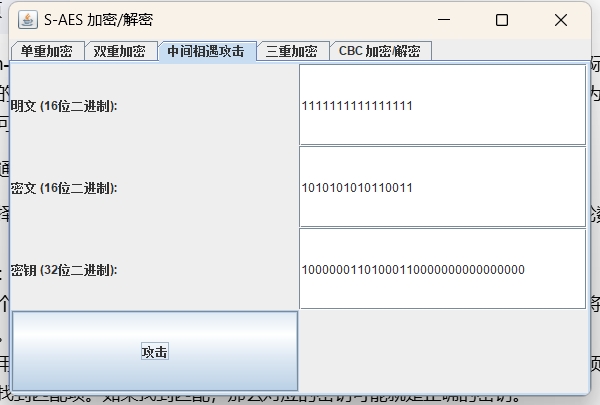
解密：





4.2 中间相遇攻击

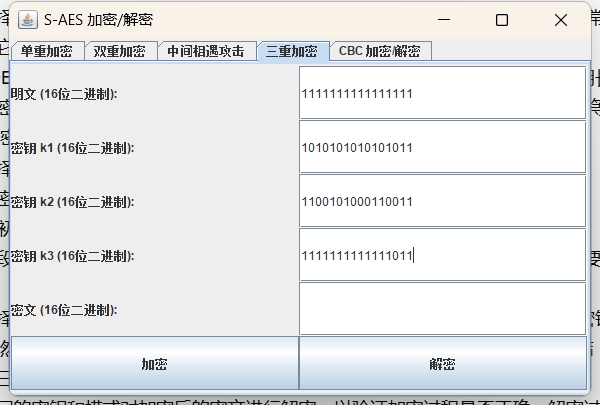
假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用中间相遇攻击的方法找到正确的密钥Key(K1+K2)。



4.3 三重加密

将S-AES算法通过三重加密进行扩展，使用48bits(K1+K2+K3)的模式进行三重加解密。

加密：





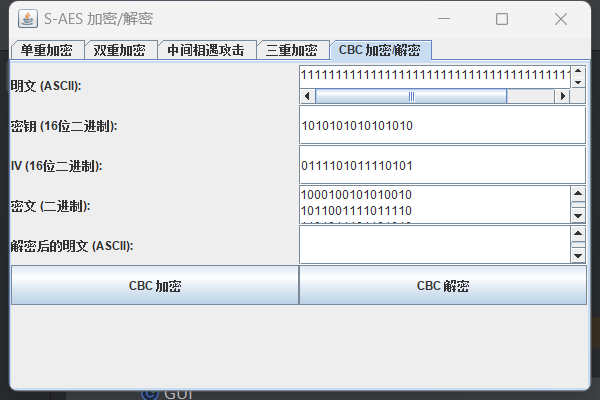
解密：



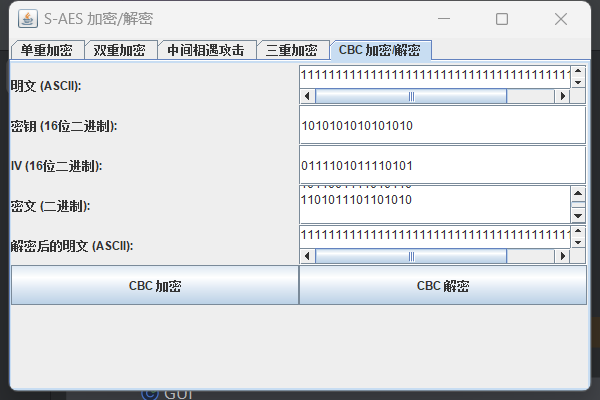
**第5关：工作模式**

基于S-AES算法，使用密码分组链(CBC)模式对较长的明文消息进行加密。注意初始向量(16 bits) 的生成，并需要加解密双方共享。在CBC模式下进行加密，并尝试对密文分组进行替换或修改，然后进行解密。

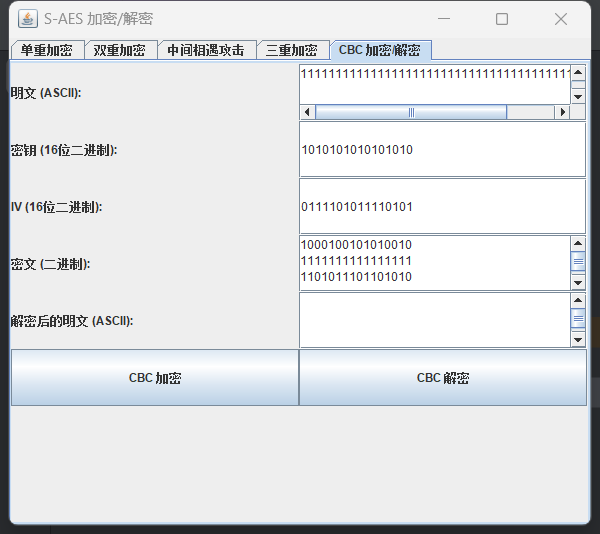
（加密）输入较长的明文和16bit的密文和IV，得到密文：

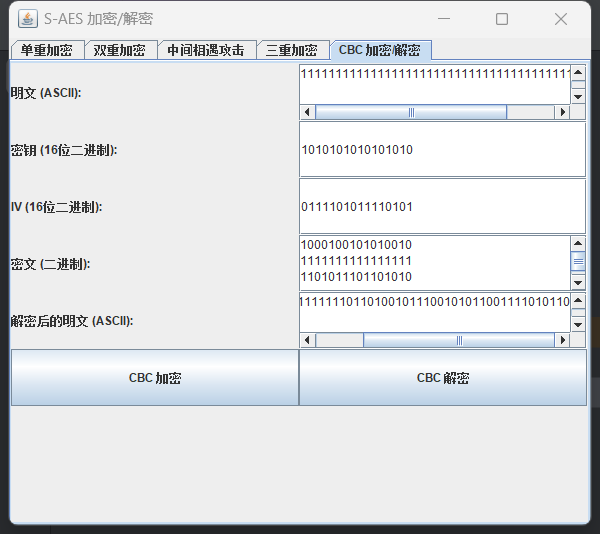


（解密）输入较长的明文和16bit的密文和IV，得到密文：

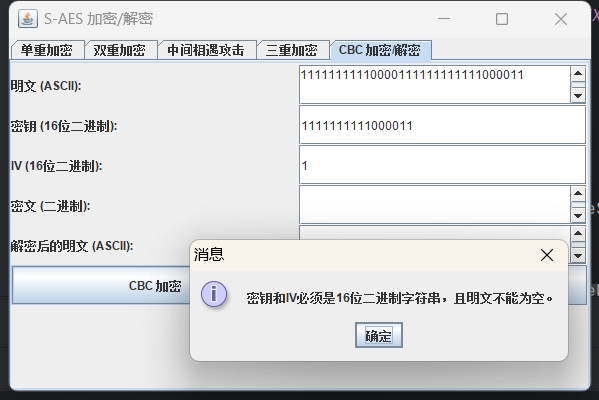
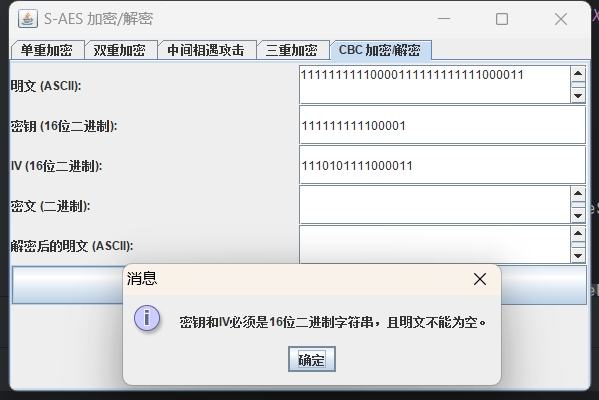


将密文进行篡改，得到结果：





如果密钥和IV输入不是16bit，会出现如下提示：



如果明文为空，会出现如下提示：

