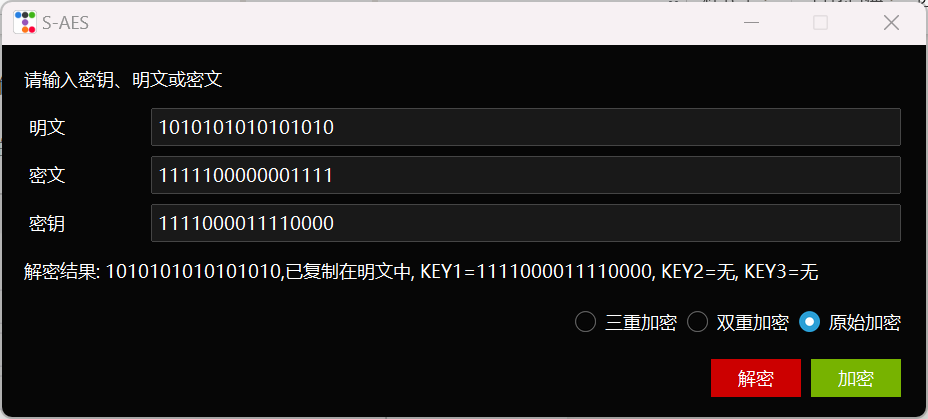
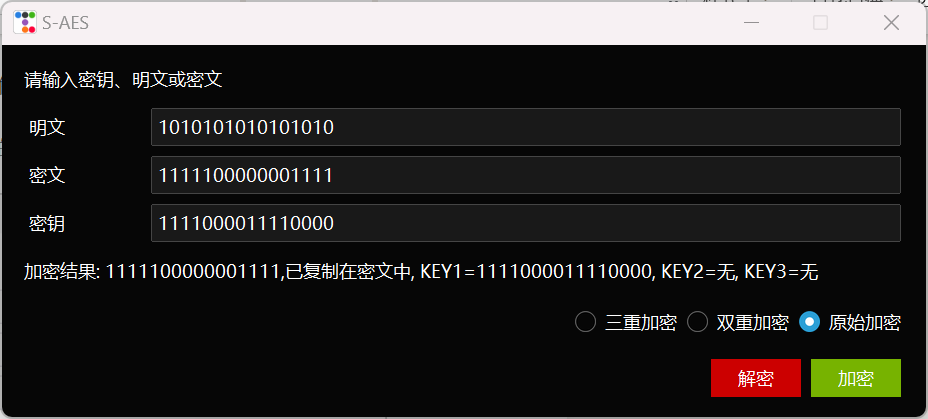
1.基本测试

根据S-AES算法编写和调试程序，提供**GUI加解密**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。



如上图所示，基于 S-AES 算法, 输入16 bit 的数据和密钥会给出16 bit 的输出。程序满足测试条件。

2.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。



组内进行交叉验证，与第一关测试比较，当使用相同的密钥和明文时，在 S-AES 加密标准下，会给出相同的密文，解密标准下，会给出相同的明文，交叉测试完成。

3.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)。



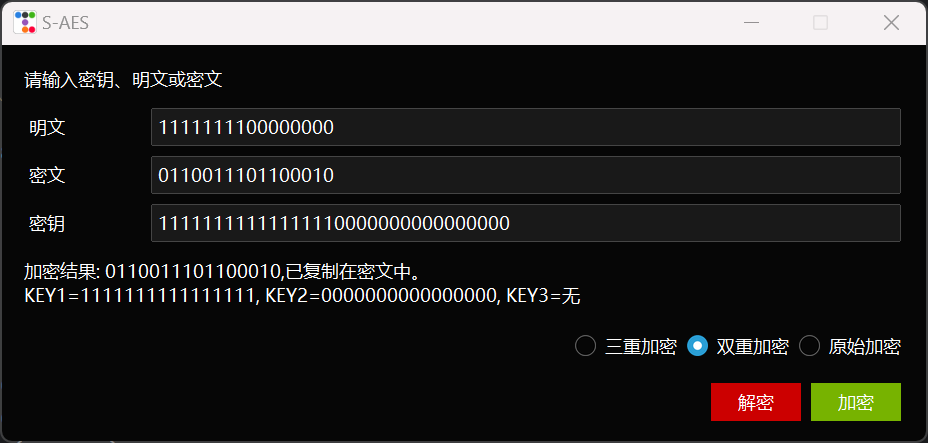
由上图可知，程序可以实现对ACII字符串的加密，满足测试要求。

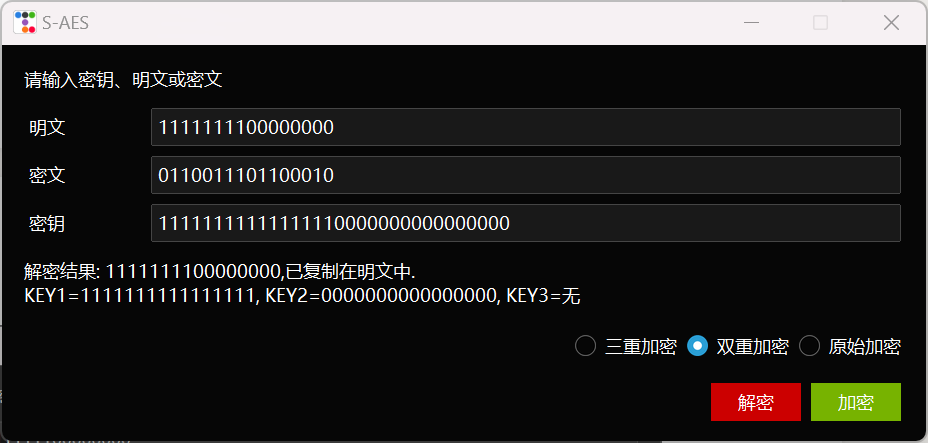


4.多重加密

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。以bit 模式进行测试，如下所示：

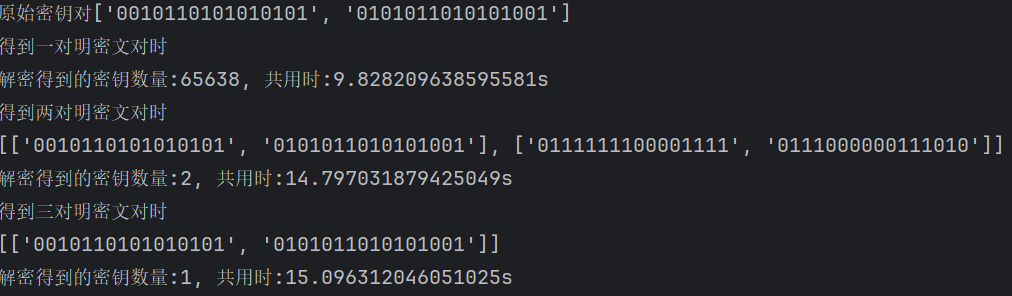




由上图可知，双重加密满足测试要求。

4.2.中间相遇攻击

假设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)。

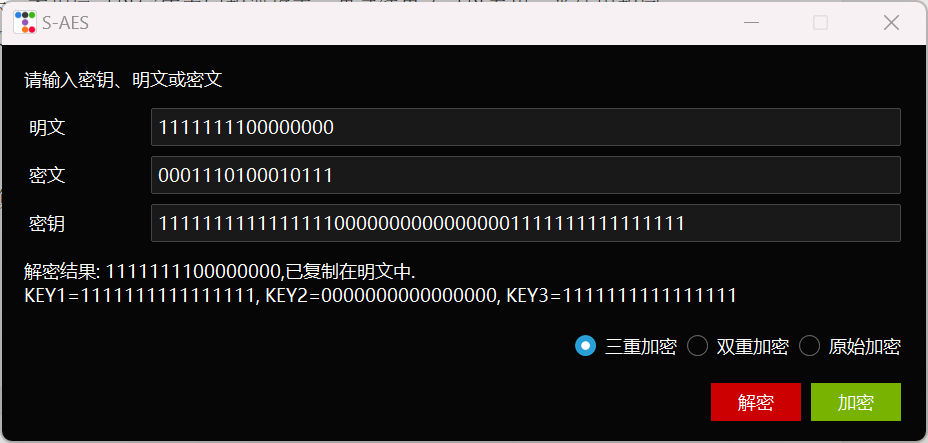
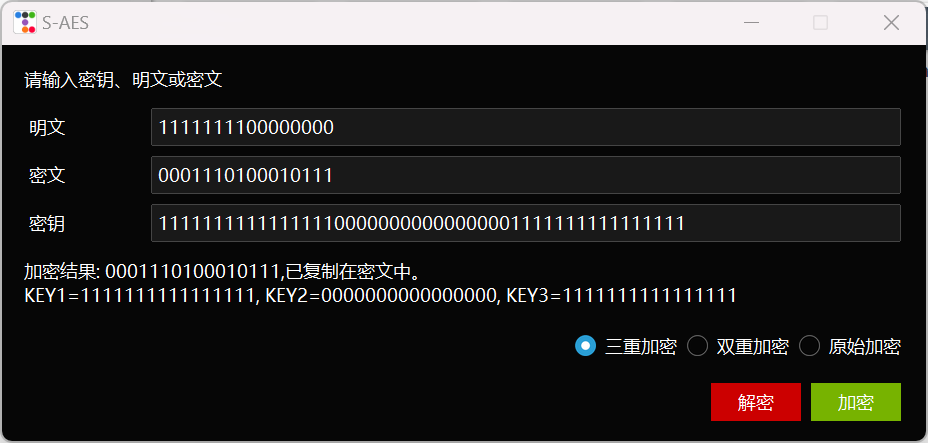


通过结果还可以看出，当使用相同密钥的一对明密文对时，密钥碰撞的现象很严重。

4.3.三重加密

将S-AES算法通过三重加密进行扩展，本程序选择下面一种模式完成：

使用48bits(K1+K2+K3)的模式进行三重加解密。



如上图所示，本程序可以完成三重加密的功能

5.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，请对比篡改密文前后的解密结果。

