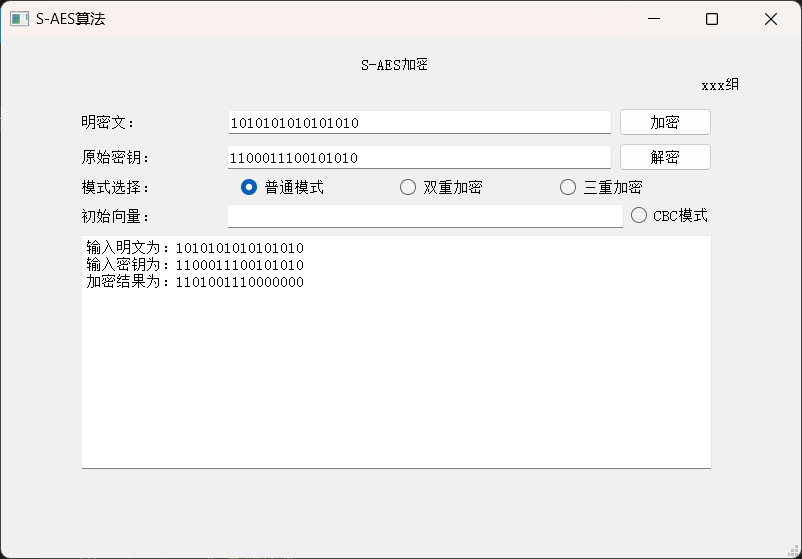
3.1 第1关：基本测试

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：1010101010101010；密钥1100011100101010；输出如图

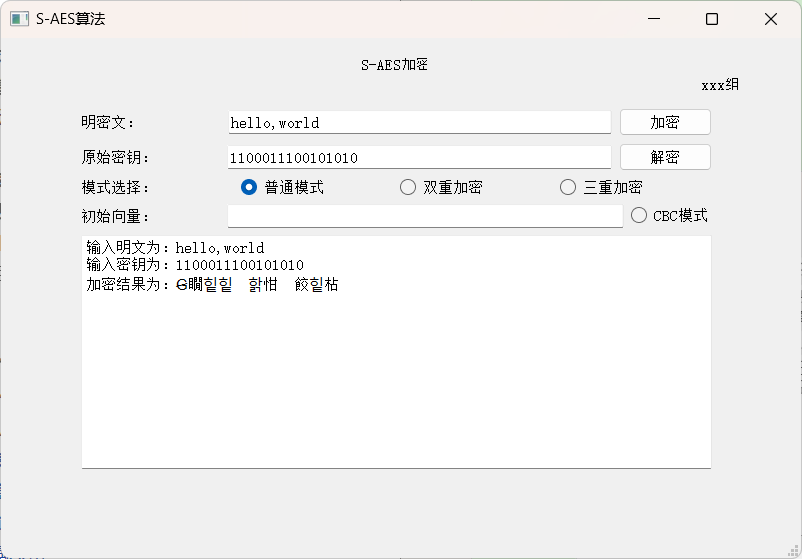


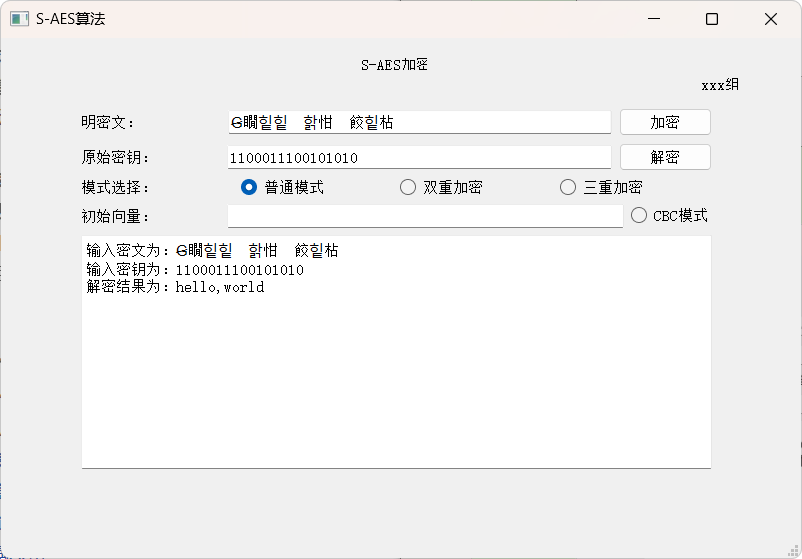
3.2 第2关：交叉测试

3.3 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)。

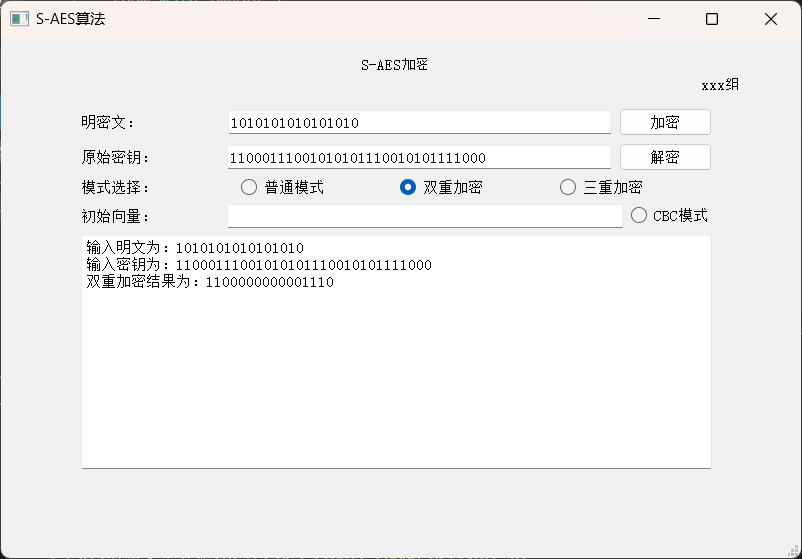
输入：hello，world

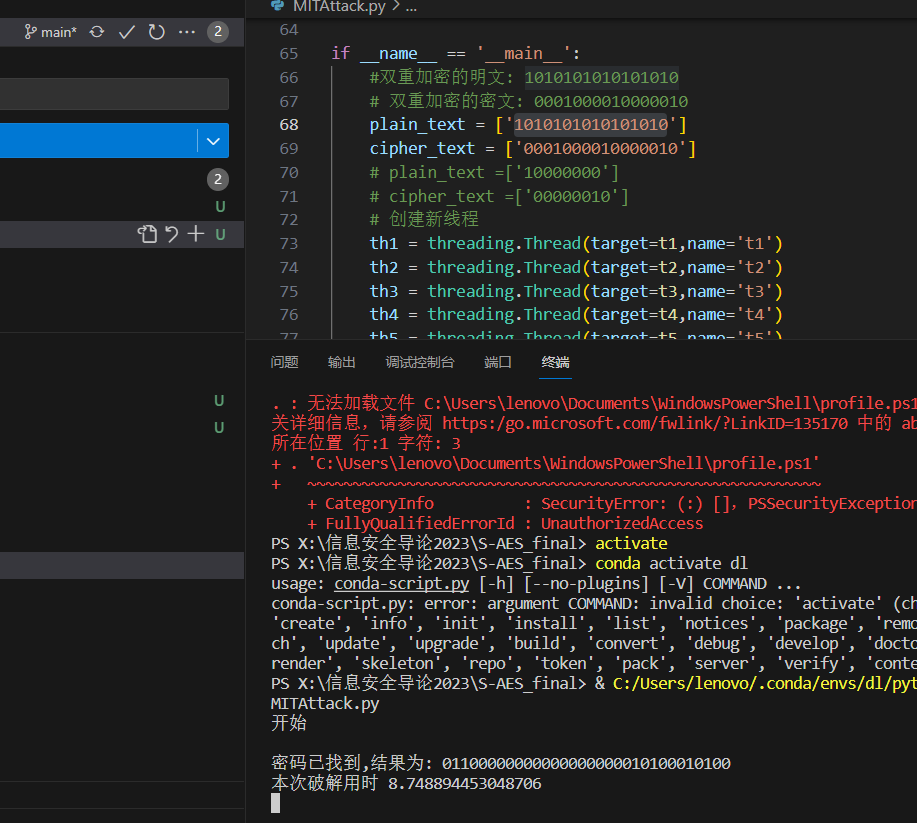




3.4 第4关：多重加密

3.4.1 双重加密

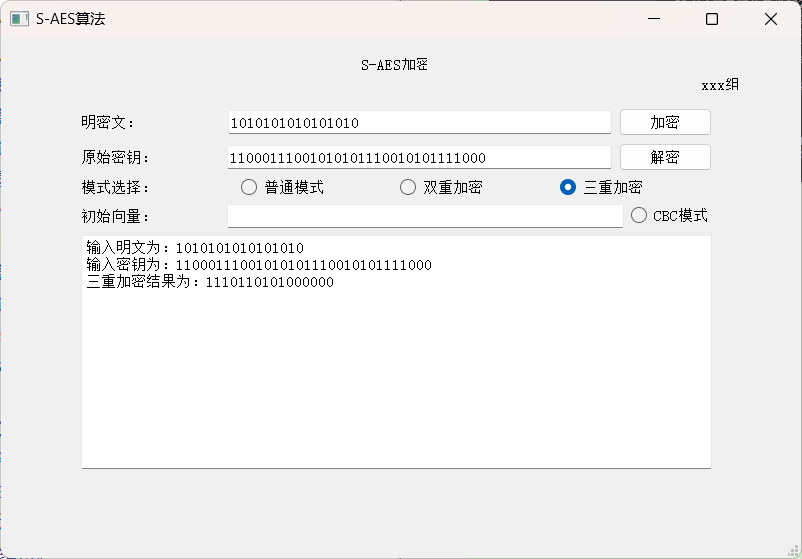


3.4.2 中间相遇攻击

3.4.3 三重加密（采用第一种方式）

输入：1010101010101010

输出：1110110101000000



3.5 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，请对比篡改密文前后的解密结果。

输入长密文：这是CBC模式的测试，需要一个较长密文

输出：如图

对应解密过程如图

