信息安全导论作业二 S-AES实现

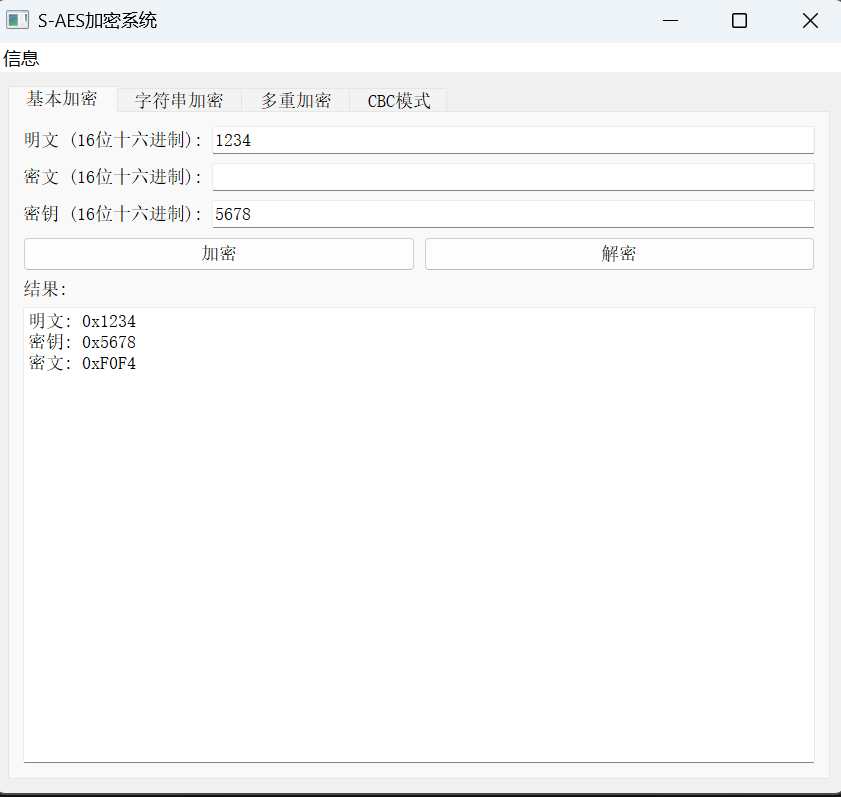
1. 作业说明

作业中使用python代码实现了一个S-AES算法，包括基本加密，字符串加密，多重加密，中间相遇攻击，CBC模式的功能。

1. 测试截图

2.1 基本加解密

基本加密：

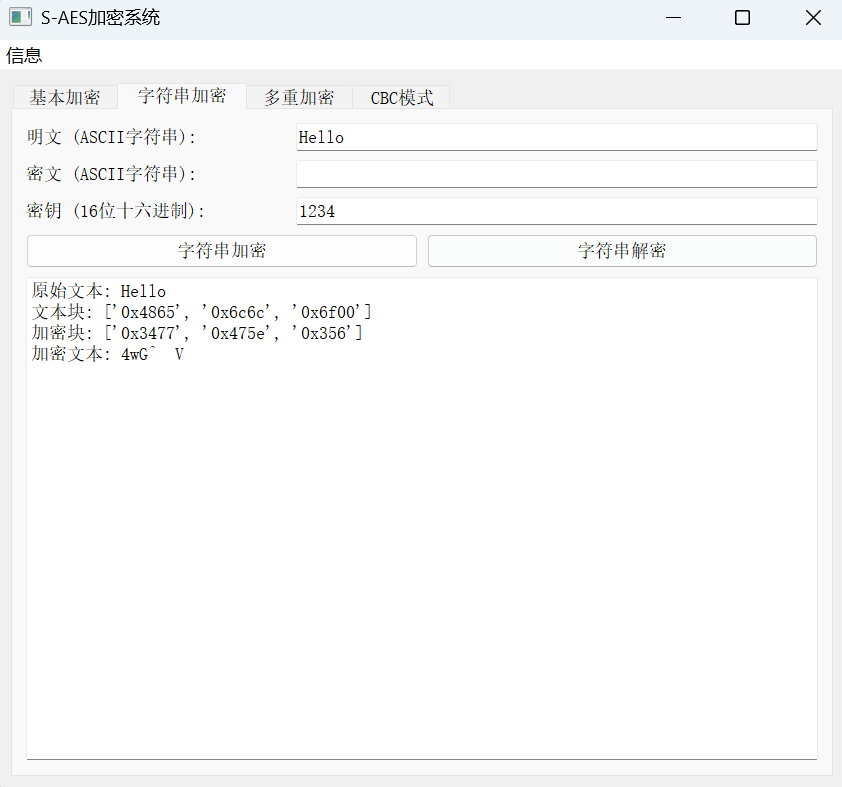


基本解密：

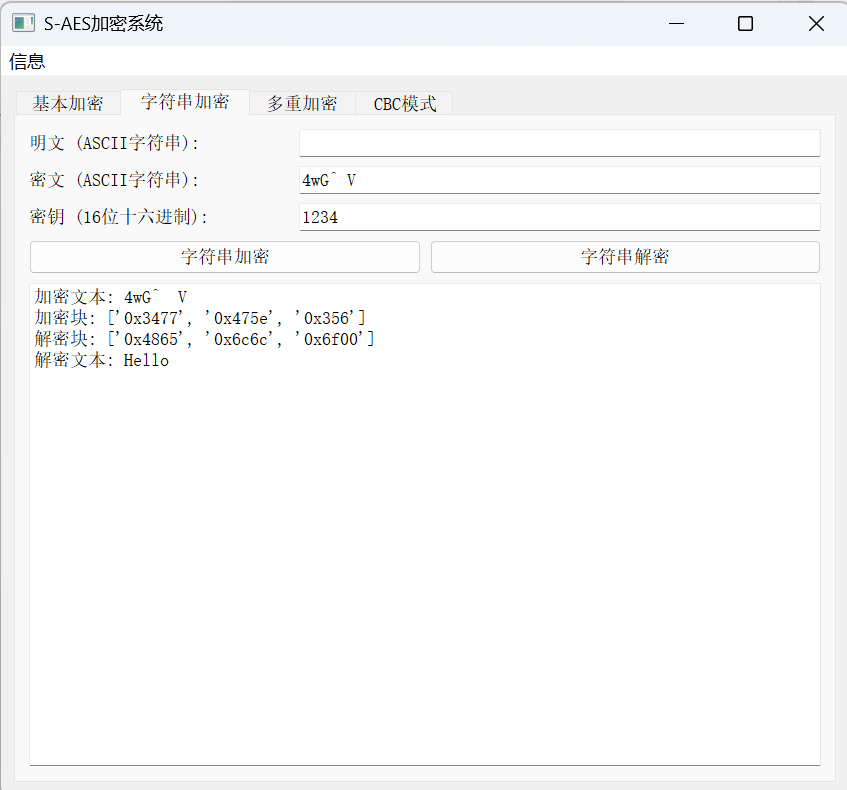


2.2字符串加解密

字符串加密：

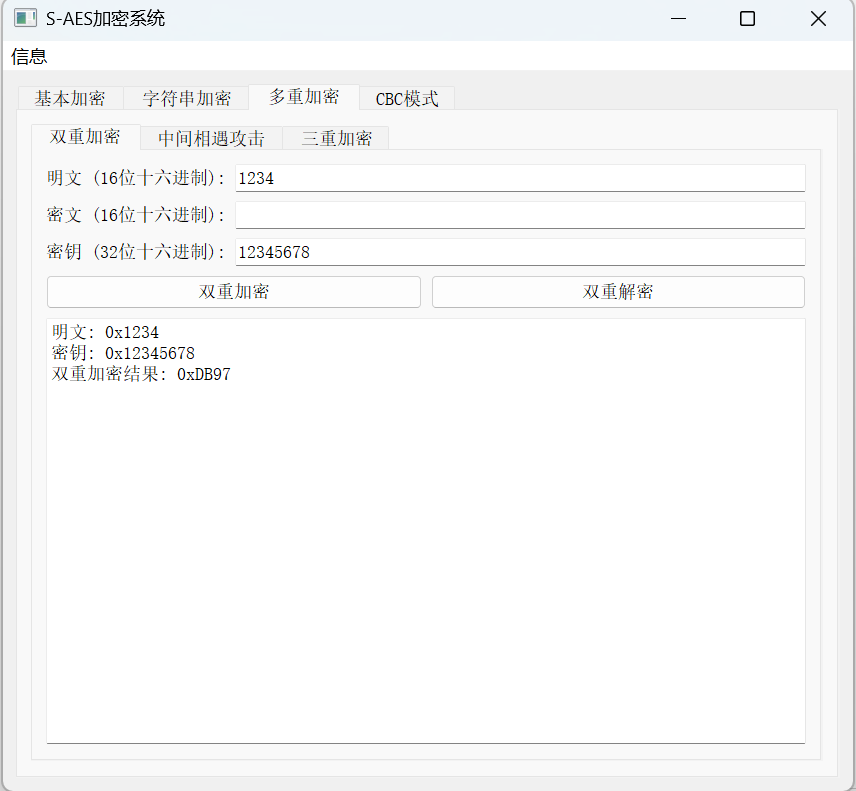


字符串解密：

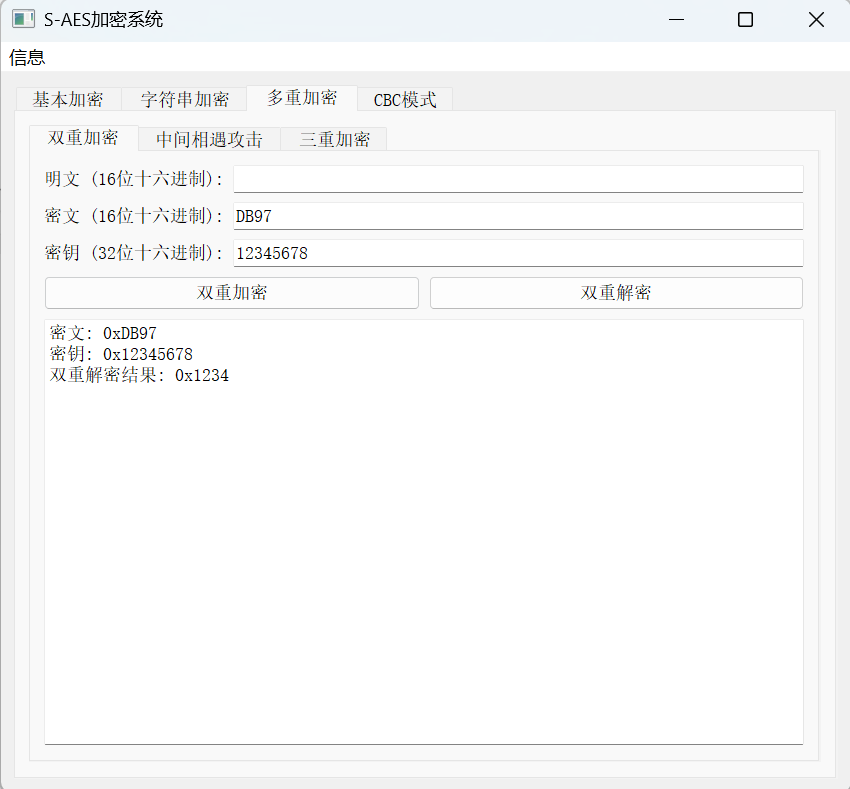


2.3多重加解密

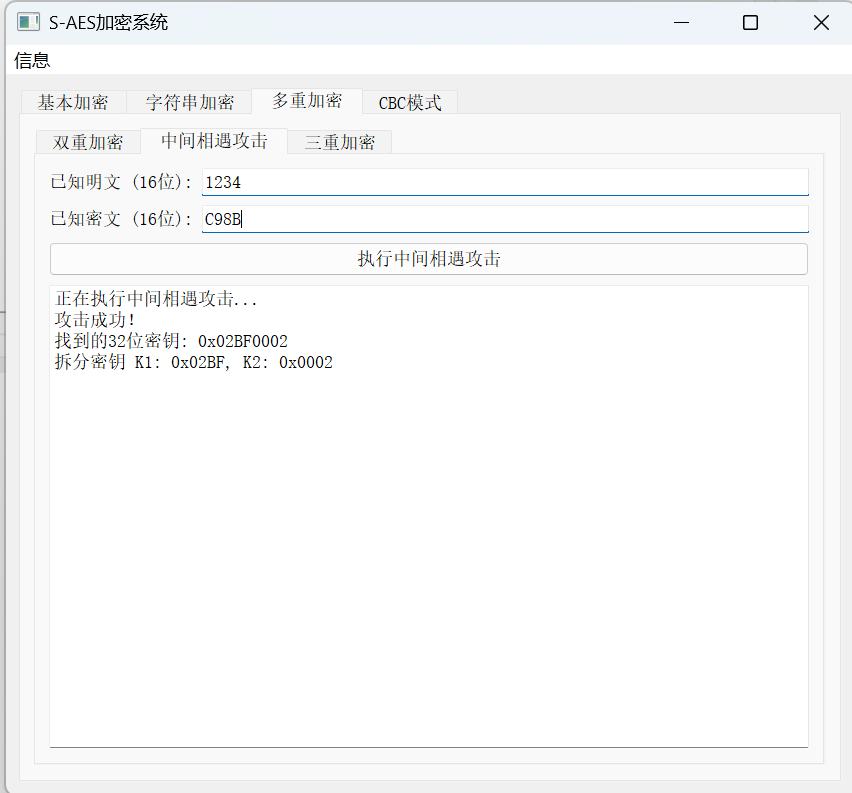
双重加密：



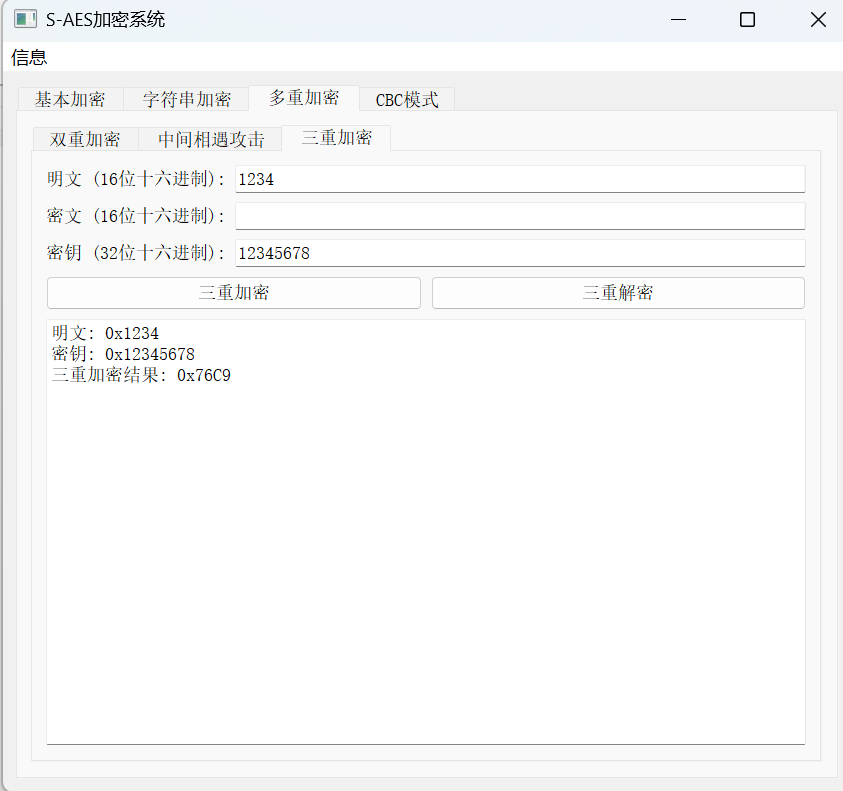
双重解密：



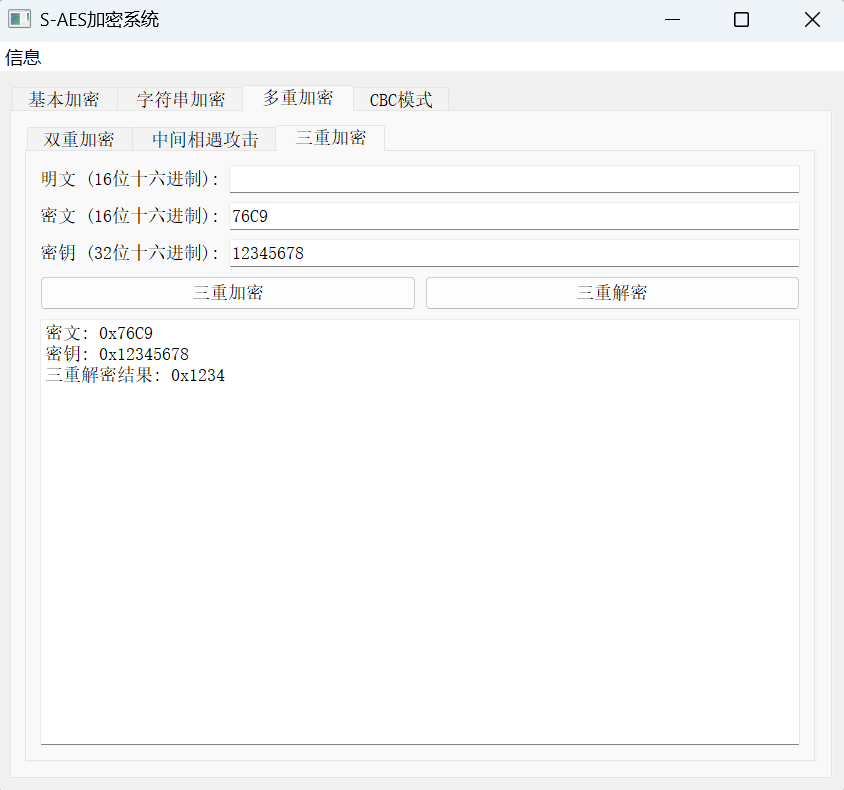
中间相遇攻击：



三重加密：



三重解密：

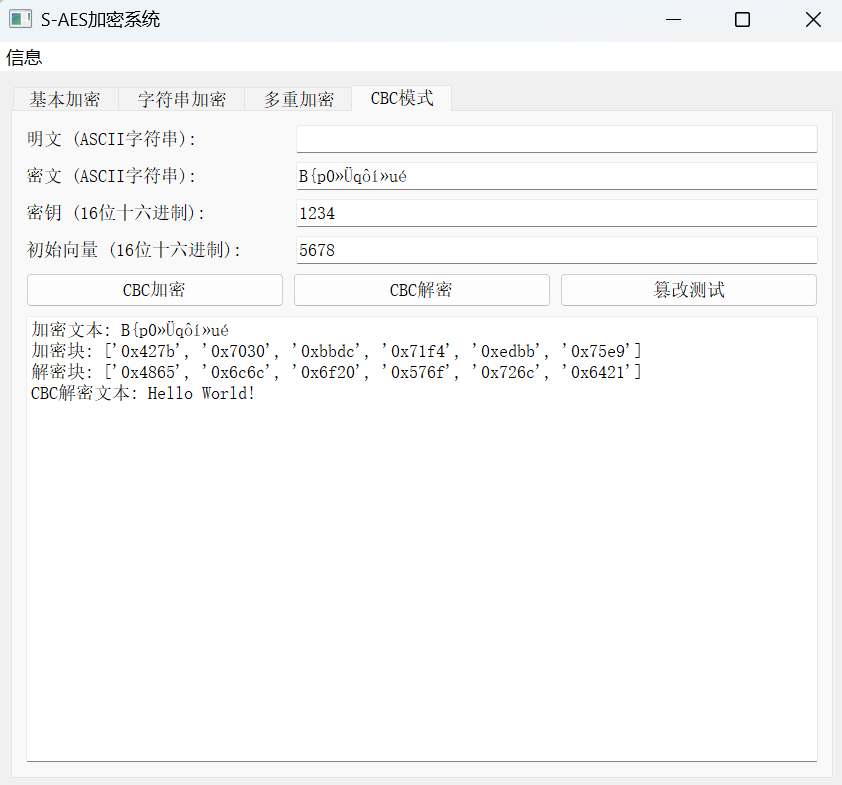


2.4 CBC模式

CBC加密：



CBC解密：



篡改测试：



1. 测试结果

3.1交叉测试

在具有相同的相同算法流程和转换单元情况下，算法在进行加解密后会得到相同的结果。

3.2中间相遇攻击测试

由2.3多重加解密中截图，中间相遇攻击可以找出符合条件的密钥K1和K2。

3.3CBC模式测试

由2.3CBC模式中截图，可以正确实现CBC模型下的加解密以及篡改测试。