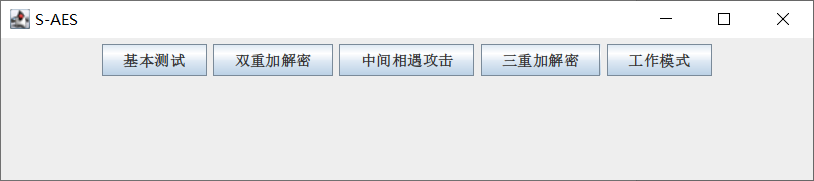
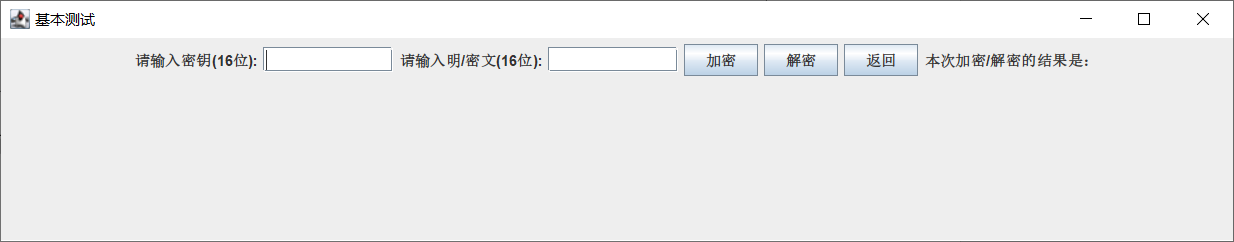
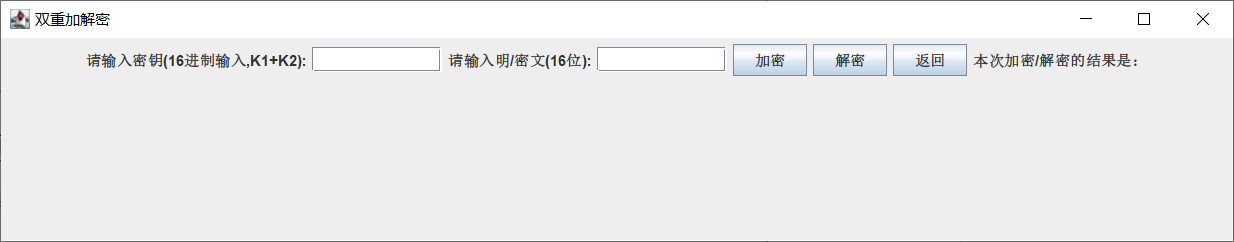
第一关：基本测试

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。

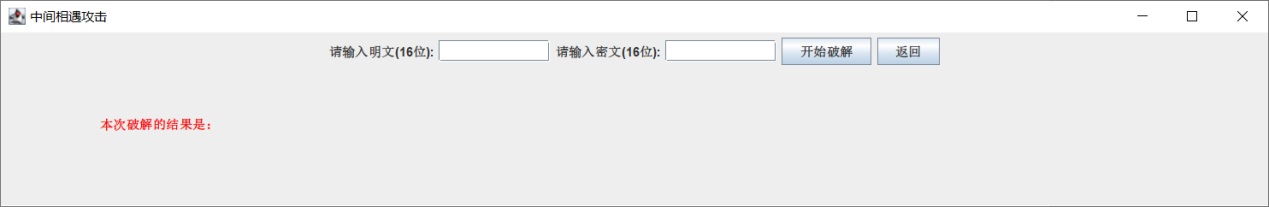
主界面

基本测试界面

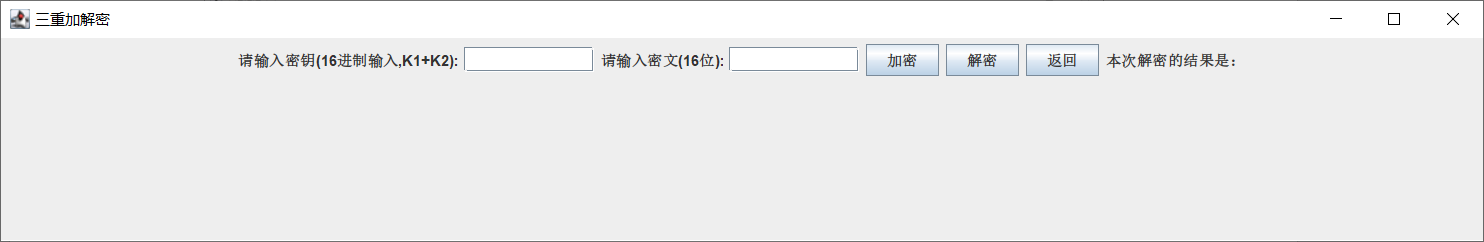
双重加解密界面



中间相遇攻击界面

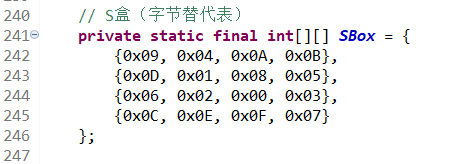


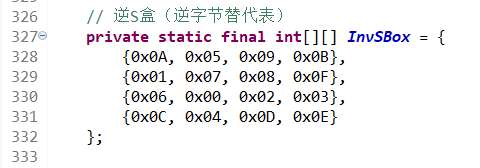
三重加解密界面

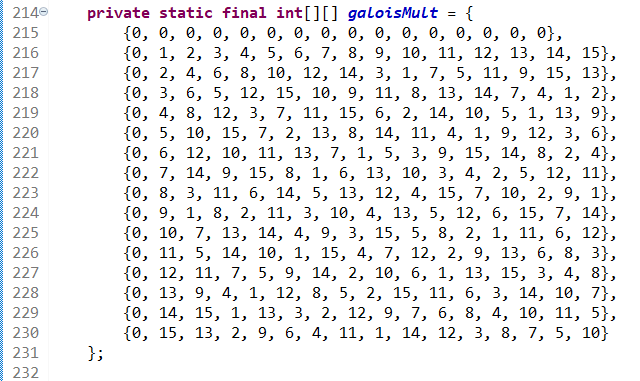


工作模式界面

第二关：交叉测试

S盒

逆S盒

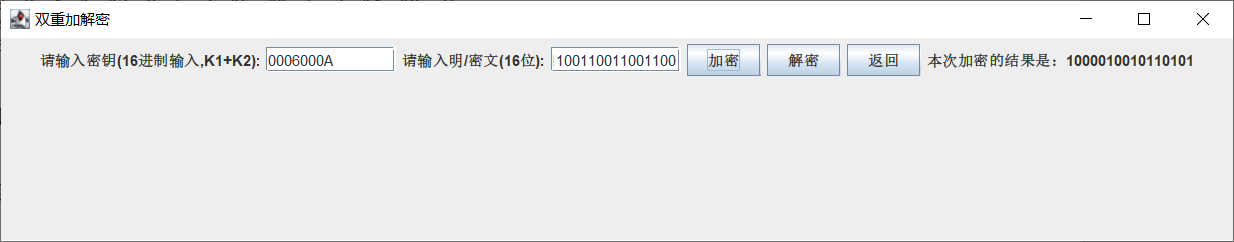
乘法表

使用了设定好的算法流程与转换单元，经过交叉测试认为完备

第四关：多重加密

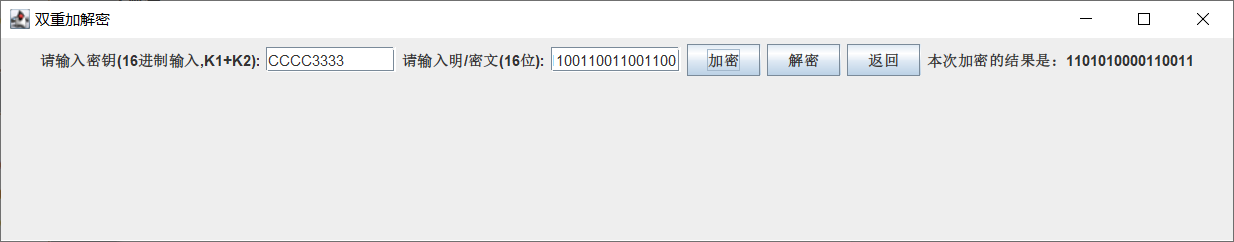
1. 双重加密

|  |  |  |
| --- | --- | --- |
| 密钥K1+K2 | 明文 | 密文 |
| CCCC3333 | 1100110011001100 | 1101010000110011 |
| 0006000A | 1100110011001100 | 1000010010110101 |



例一：

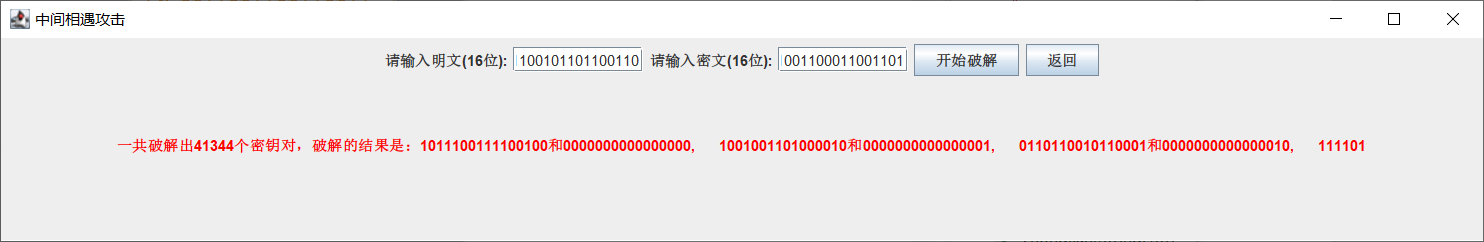
例二：



1. 中间相遇攻击

使用map将首次遍历后的中间明文和K1存储，再使用中间密文在map中寻找是否有相等的中间明文，如果有，则输出K1和K2

例一：

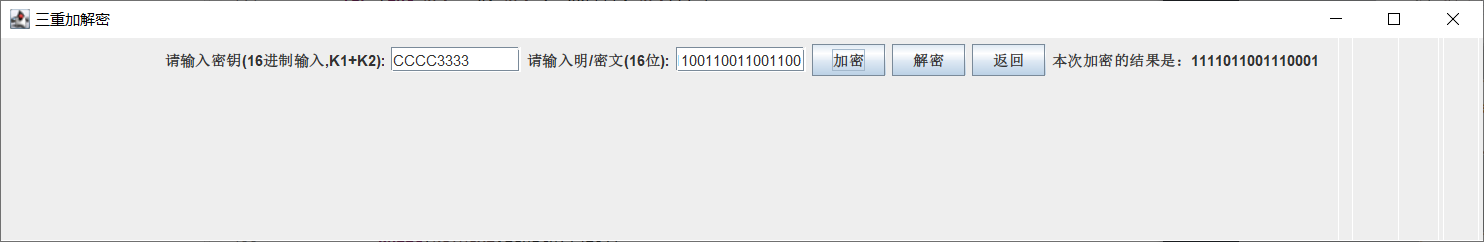


1. 三重加密

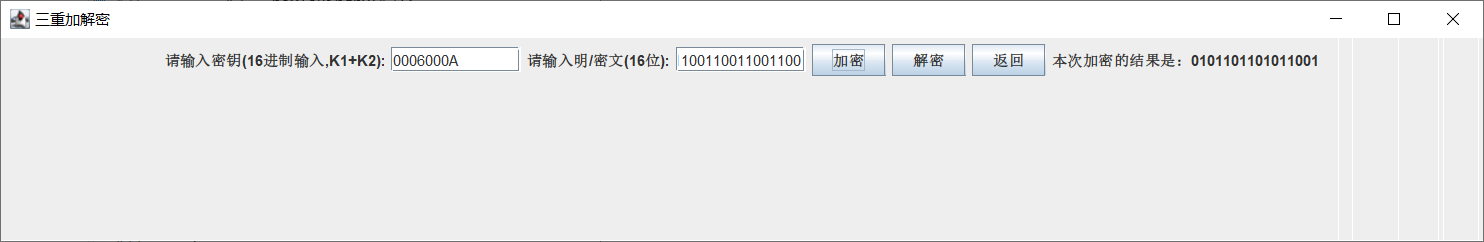
使用C = E(K1, D(K2, E(K1, P)))方案

|  |  |  |
| --- | --- | --- |
| 密钥K1+K2 | 明文 | 密文 |
| CCCC3333 | 1100110011001100 | 1111011001110001 |
| 0006000A | 1100110011001100 | 0101101101011001 |

例一：



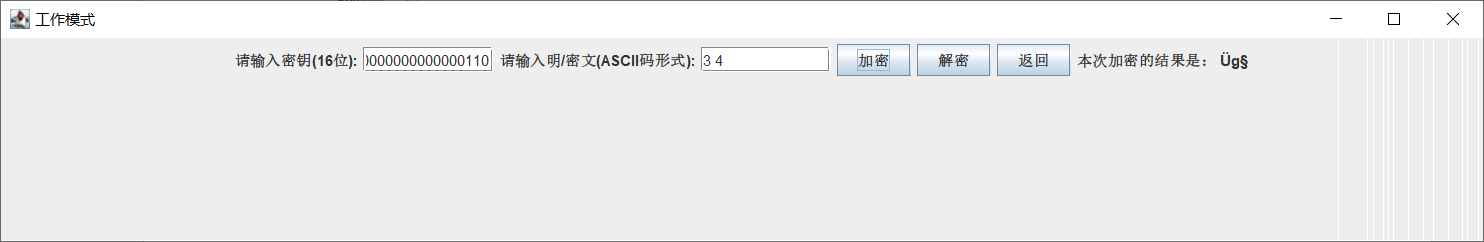
例二：



第五关：工作模式

输入ASCII明密文，输出结果为ASCII，可能为乱码

例一：



例二：

