任务一：

根据 S-DES 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 8bit 的密文。展示二进制下的基本功能：

字符文本下的基本功能测试：

任务二：

本算法已与多组同学（魏鹏坤组、方珩组、朱清扬组）进行共同测验，并检验通过。

任务三：

多重加密测试（先后展示双重加密和三重加密）

三重加密：

任务四：

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)。

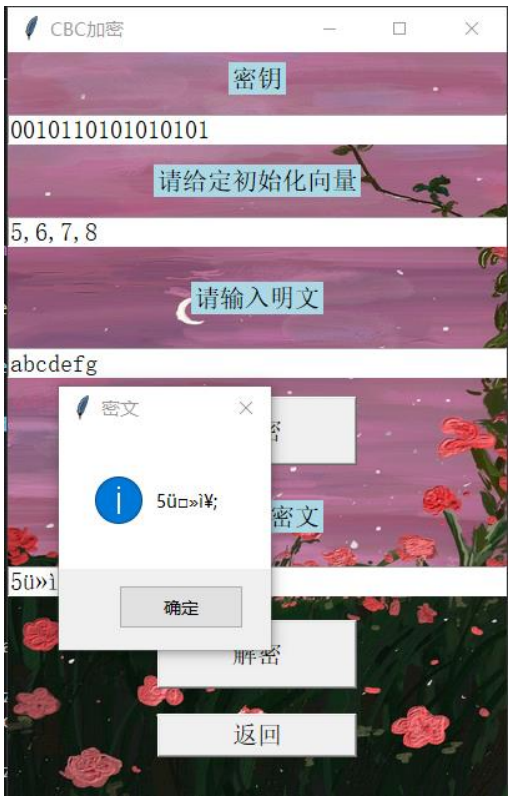
以任务三中所用到的加解密之后的明密文对（pla=[10,4,7,9],cip=[7,3,2,14]）为例，展示暴力破解找到密钥的时间以及部分密钥对，由于密钥对过多，仅展示第一个密钥与原始的第一个密钥相同的情况。

破解所需要的时间为 7.012970209121704s，找到的符合条件的 key 有以下四组结果。

```
破解时间：  7.012970209121704
[2, 13, 5, 5] [0, 10, 10, 0]
[2, 13, 5, 5] [0, 15, 0, 15]
[2, 13, 5, 5] [4, 14, 9, 5]
[2, 13, 5, 5] [6, 2, 2, 9]
```

任务五：

以加密明文为“abcdefg”为例先展示基本加解密功能。



现在改变密文分组后在进行解密测试：

可以发现在改变明文顺序后，由于通过密码链模式进行加密，改变之后的部分和改变之

前的部分完全不一样，这一点与 Ascii 编码下的加解密模式有所不同。