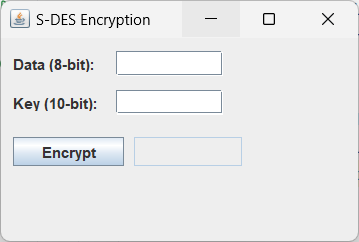
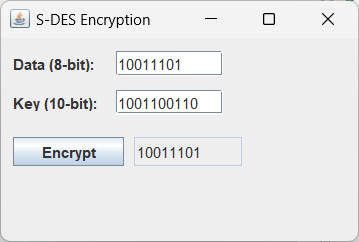
**第一关：基本测试**

初始ui：



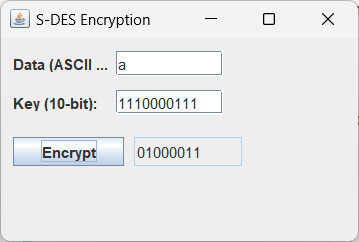
对输出bit位进行固定，使其在不足8位时自动补足8位，解密时的展示：



**第二关：交叉测试**

**第三关：扩展功能**

修改识别功能以及ui界面后实现对ASCII输入明文的解密

****

**第四关：暴力破解**

密钥：1011011011

明文密文对：

01110100 11011100

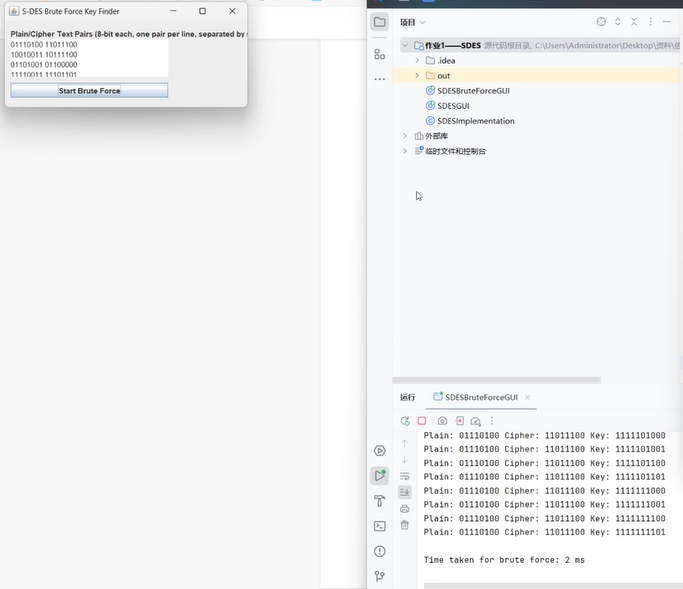
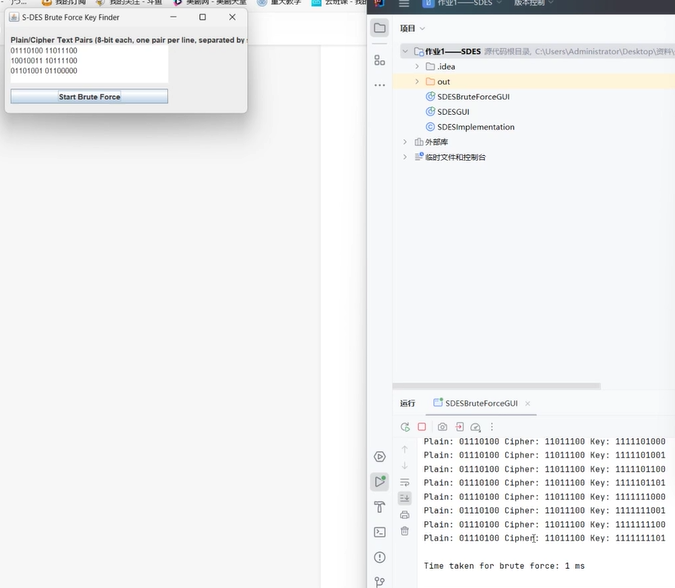
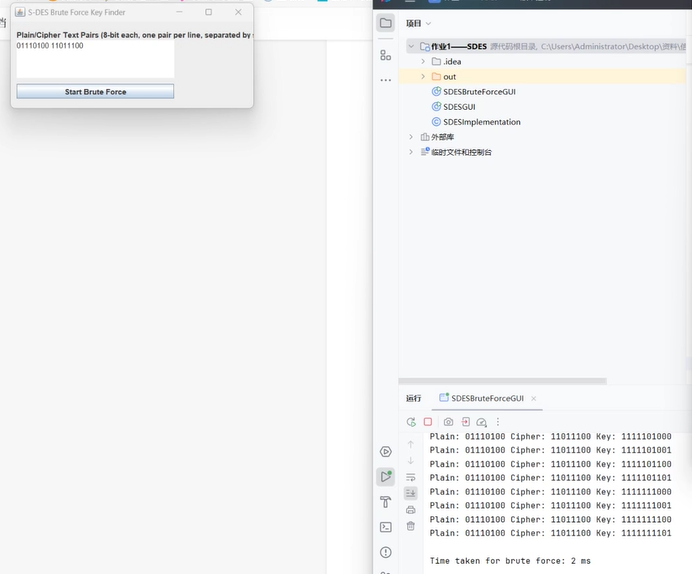
10010011 10111100

01101001 01100000

11110011 11101101

10110000 11001100

由于bit位较少，因此遍历的时间普遍较短，如图：



具体操作可以参考文件中的视频：《暴力破解》

**第五关：封闭测试**

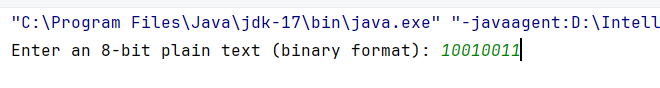
在S-DES（简化版的数据加密标准）算法中，理论上是存在不同密钥加密同一明文得到相同密文的情况，这被称为弱密钥或相关密钥攻击。

弱密钥：

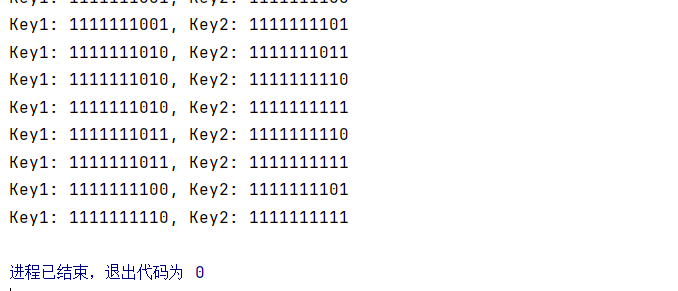
在S-DES中，如果存在一对密钥 KiKi和 KjKj​（其中 Ki≠KjKi=Kj），使得对于某个明文 PP，使用这两个密钥加密得到相同的密文 CC，那么这对密钥就被称为弱密钥。形式上，如果： EKi(P)=EKj(P)=CEKi​​(P)=EKj​​(P)=C 那么 KiKi 和 KjKj 就是弱密钥。

以下为检测弱密钥的测试结果：

测试明文：10010011



部分输出：



具体操作可以参考文件中的视频：《检测弱密钥》