测试结果

1. 第1关：基本测试

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8bit的数据和10bit的密钥，输出是8bit的密文。

**加密部分：**





**解密部分：**





1. 第2关：交叉测试

目前本组已经和其他多组完成了交叉测试，经过验证在使用相同的密钥对相同的输入进行加密或解密时，得到的结果均一致。因此本组的SDES算法实现满足算法标准，满足了算法流程和转换单元(P-Box、S-Box等)，保证了算法和程序在异构的系统或平台上都可以正常运行。

交叉测试1：

测试用例a：明文为10101010

密钥为1111100000

密文为00111011





交叉测试2：

测试用例b：明文为10011010

密钥为1010000010

密文为11101111



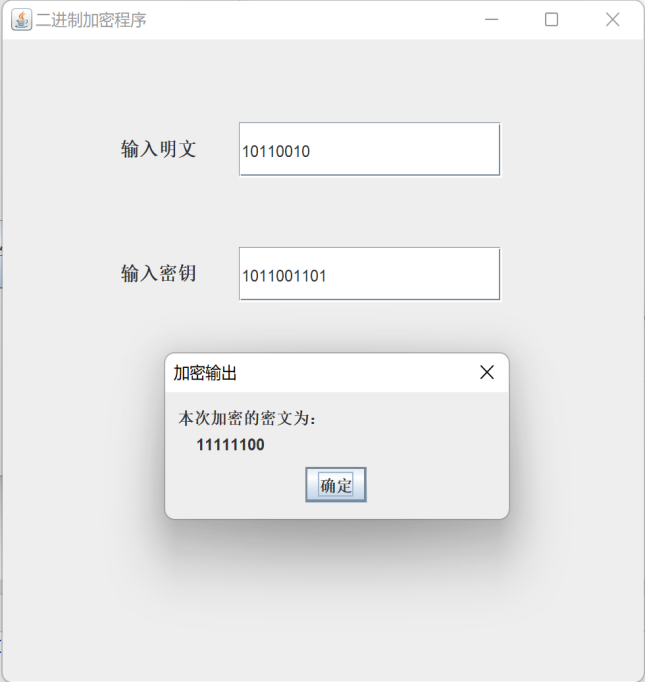
 ****

测试用例c：明文为10110010

密钥为1011001101

密文为11111100



**** 

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。要实现对ASCII编码字符串的加密解密，首先要把字符串中的每个字符分别先转化为10进制数再转化为8位二进制数，然后逐一进行加密解密。

**加密部分：**





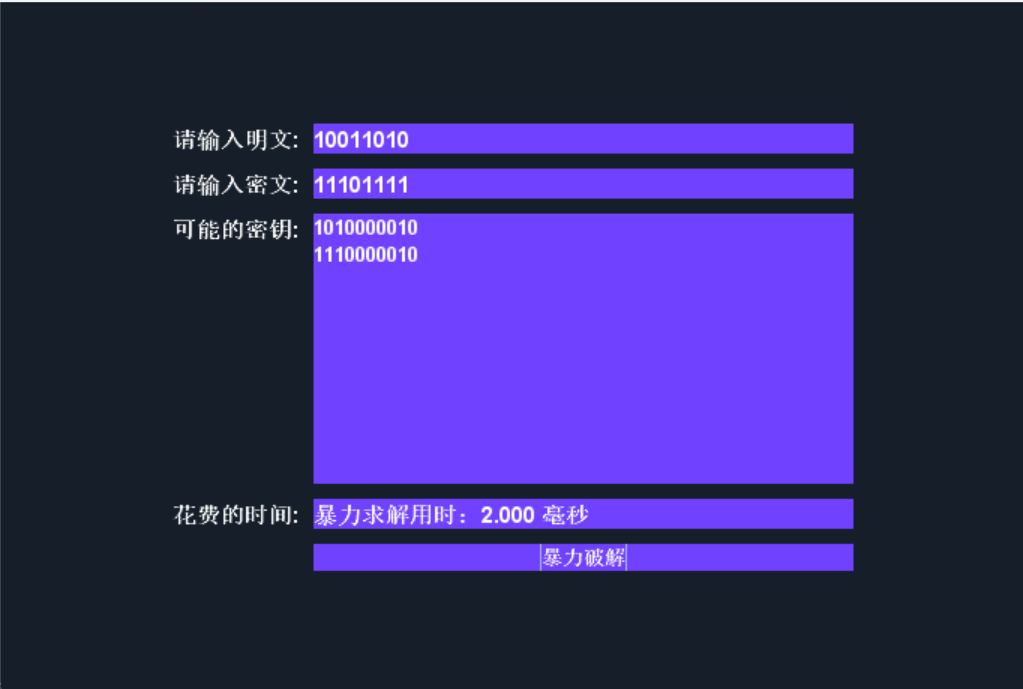
**解密部分：**

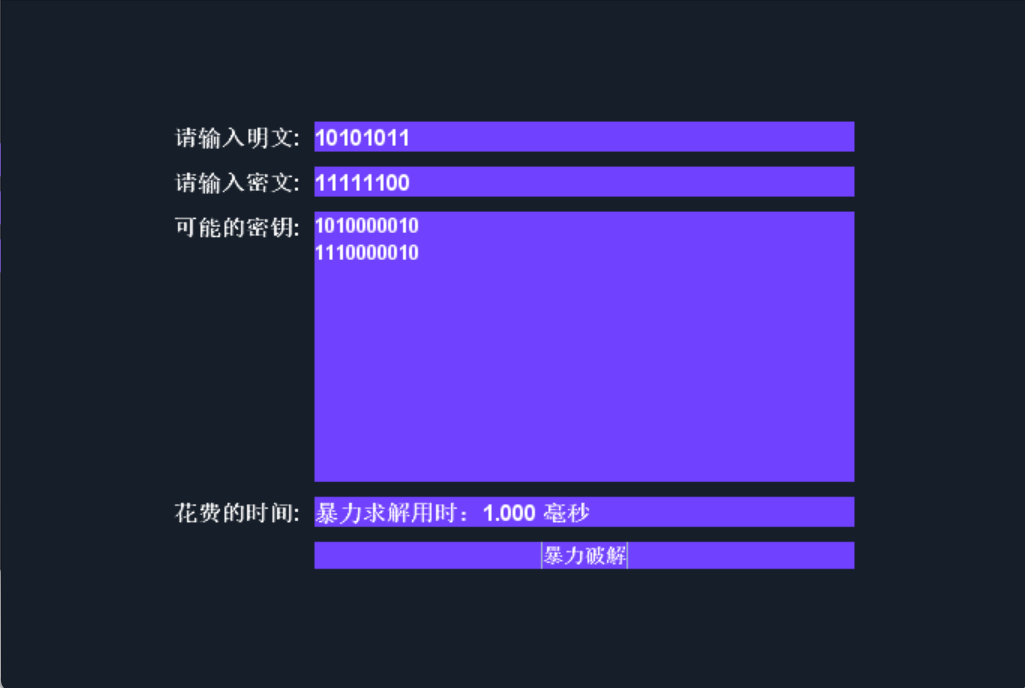


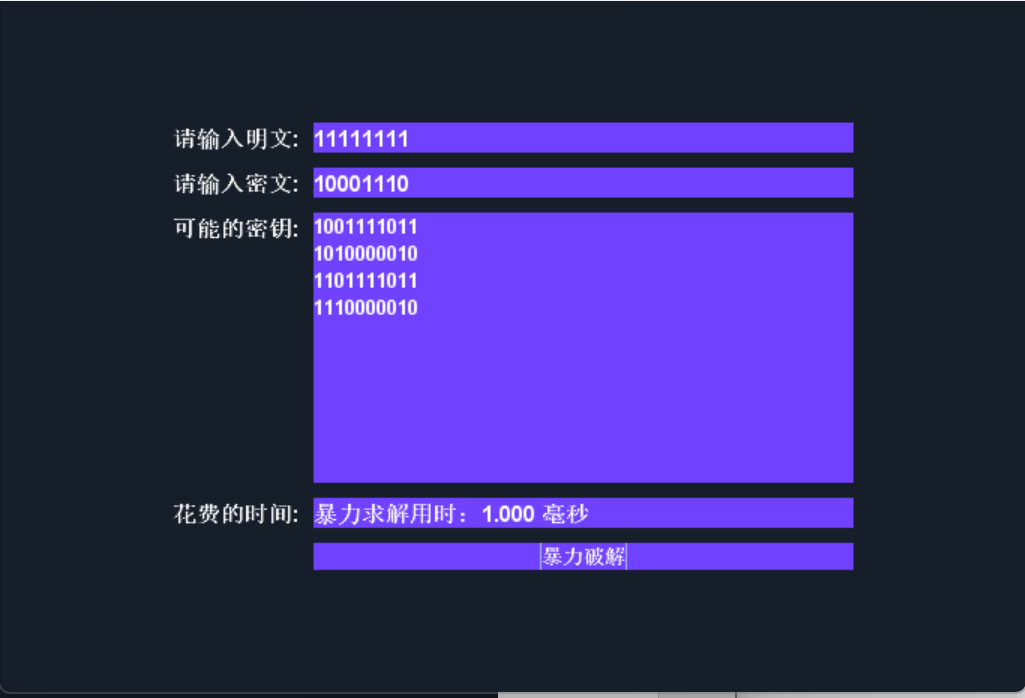


4. 第4关：暴力破解

假设你找到了使用相同密钥的明、密文对，请尝试使用暴力破解的方法找到正确的密钥Key。在编写程序时，你也可以考虑使用多线程的方式提升破解的效率。请设定时间戳，展示你在多长时间内完成了暴力破解。以下是对三个具有相同密钥的明密文对的破解。







5 .第5关：封闭测试

根据第4关的结果，进一步分析，对于你随机选择的一个明密文对，是不是有不止一个密钥Key？进一步扩展，对应明文空间任意给定的明文分组P\_{n}，是否会出现选择不同的密钥加密得到相同密文的情况？

**答：**由第4关的结果可知，随机选择一对明密文对，它们之间可能存在多个密钥，如上图。因此，在明文空间任意给定的明文分组内，会出现不同密钥加密获得相同密文的情况。