测试结果

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。

测试：

加密操作

1、输入需要加密的 8bit 明文和 10 位二进制密钥。

2、点击“加密”按钮，结果将显示在“输出结果”框中：

3、加密结果为二进制数字。

图 1　8 位二进制模式下的加密模式

解密操作

1、选择输入模式为 8 位二进制。

2、输入要解密的二进制密文。

3、输入 10 位二进制密钥。

4、点击“解密”按钮，结果将以二进制格式显示。

图 2　8 位二进制模式下的解密模式

加密与解密的明密文对相同。

第 2 关：交叉测试

考虑到是**算法标准**，所有人在编写程序的时候需要使用相同算法流程和转换单元(P-Box、S-Box 等)，以保证算法和程序在异构的系统或平台上都可以正常运行。

设有 A 和 B 两组位同学(选择相同的密钥 K)；则 A、B 组同学编写的程序对明文 P 进行加密得到相同的密文 C；或者 B 组同学接收到 A 组程序加密的密文 C，使用 B 组程序进行解密可得到与 A 相同的 P。

测试：

经过与高俪洪组的交叉测试，能够得到相同的明文和密文

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(分组为 1 Byte)，对应地输出也可以是 ACII 字符串(很可能是乱码)。

测试：

1、选择输入模式为 ASCII 模式。

2、输入要加密的二进制明文。

3、输入 10 位二进制密钥。

4、点击“加密”按钮，结果将以 ASCII 字符显示。

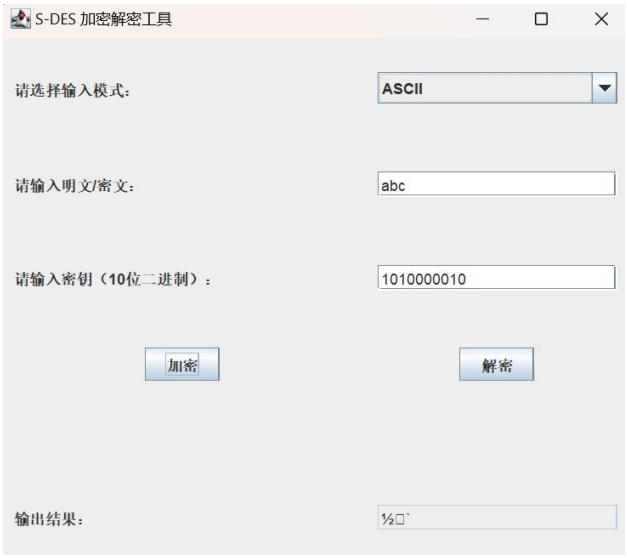

图 3 ASCII 模式下的加密模式

第 4 关：暴力破解

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，用视频或动图展示你在多长时间内完成了暴力破解。

测试：

通过暴力破解测试发现可以在相当短的时间内找到密钥

```
请输入明文（8位二进制数）：10011010
请输入密文（8位二进制数）：01101011
[==                                                  ] 4%找到匹配的密钥：0001001100
[=======                                             ] 14%找到匹配的密钥：0011001000
[=======================                             ] 44%找到匹配的密钥：0111010111
[================================                    ] 64%找到匹配的密钥：1010011101
[=========================================           ] 74%找到匹配的密钥：1100000110
[============================================        ] 84%找到匹配的密钥：1110000010
[================================================== ] 99%
破解时间：2259 毫秒
总延时：2240 毫秒
```

几乎是 20 毫秒就找到了所有符合要求的密钥，这是一个相对短的时间，可见简要版 des 算法的加密安全性不是很高。

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 K_{i}\ne K_{j}加密得到相同密文 C_n 的情况？

根据第四关的结果，很显然每一对明密文之间不止一组密钥，在我测试的那一组里，有六把密钥，经进一步测试发现，六把密钥全都符合，所以同样的明文都通过不同的密钥加密成了相同的密文，所以第二问的答案也很显然是肯定的。