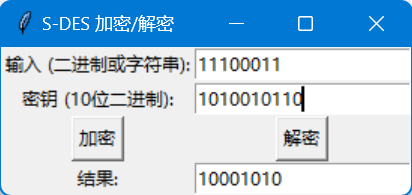
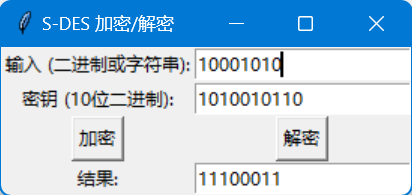
第一关：基本测试

加密测试：



解密测试：

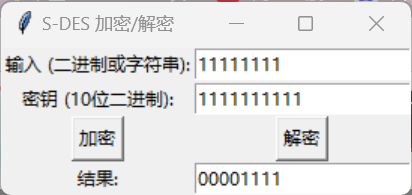


第二关：交叉测试

加密测试

明文：11111111

密钥：1111111111



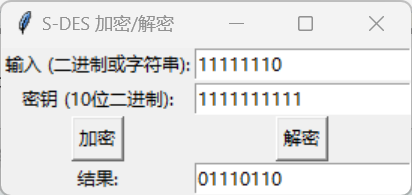
其它组

****

解密测试

密文：11111110

密钥：1111111111



其它组：



第三关：扩展功能

加密



解密



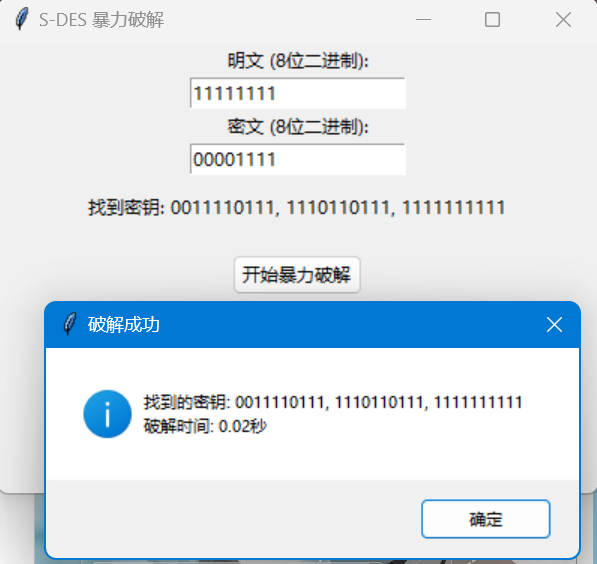
第四关：暴力破解

暴力破解的思路：

由于S-DES密钥长度是10位，所以暴力破解的密钥空间是，这可以通过遍历所有可能的密钥来解密密文，然后与已知的明文进行比对，来判断是否正确。

原理：

生成所有的密钥，使用每个密钥对密文进行解密，得到的明文与已知的明文匹配，直到所有密钥都测试完毕。



第五关：封闭测试

1. 明文-密文对是否存在不止一个密钥？

对于随机选择的一个明文-密文对，很有可能存在不止一个密钥能够加密得到相同的密文。这是因为某些加密算法的设计存在密钥重合的现象，即密钥空间远大于明文空间，从而在加密过程中可能会出现多个密钥映射到同一个密文的情况。

这在较小密钥长度的加密算法（如 S-DES）中尤其常见，原因如下：

1. S-DES 的密钥空间大小为种可能的密钥。
2. 明文和密文的长度均为 8 位，因此明文和密文空间大小为种可能。

这说明，可能平均每对明文-密文对有4个密钥能产生相同的密文。

2.对应任意明文分组，是否会出现不同密钥加密得到相同密文的情况？

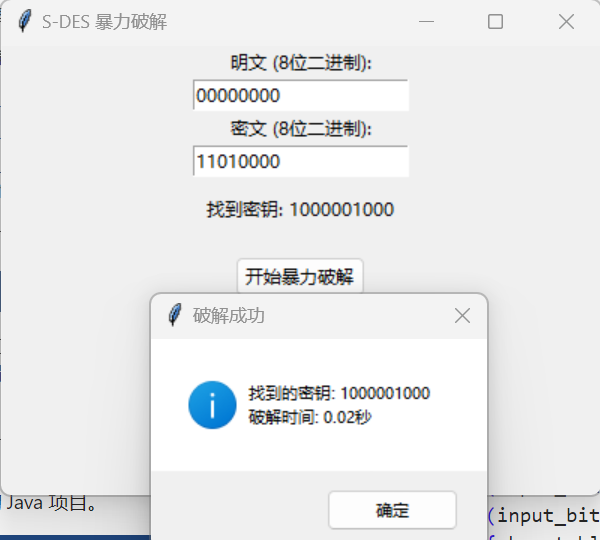
根据上面分析，对于S-DES算法，存在多个密钥映射到相同的密文是必然的。

于是，应探究是否存在这么一对“明文-密文”对，有且仅有一个密钥。

编写代码并运行测试得到：



使用3.4的暴力破解，验证其密钥是否唯一



因此，对于随机选择的明密文对，有极小可能只有一个密钥Key。