**S-DES加密算法测试结果**

1. 基本测试
   1. GUI解密交互界面
      1. 加密信息以及解密信息（8bit）
      2. 密钥（10bit）



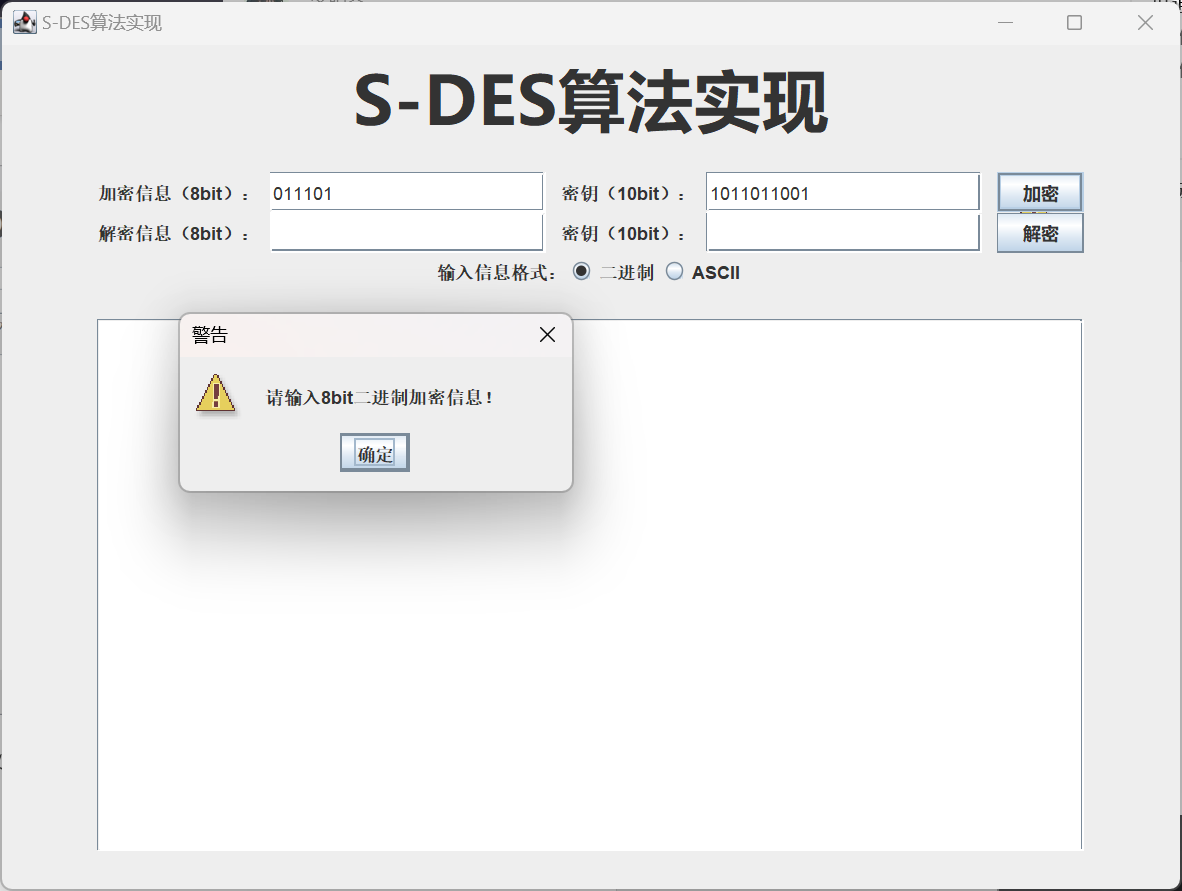
* 1. 8bit的数据加解密功能

使用密钥1011011001对明文01110100加密并解密



* 1. 输入加密信息不符合要求

使用密钥1011011001对明文011101加密并解密



结果可见，同密钥加密得到的密文使用同密钥解密后得到的明文与最初值相同，而输入格式不对时提醒错误，基本测试通过。

1. 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。

我们与**常子昕组**进行了交叉测试

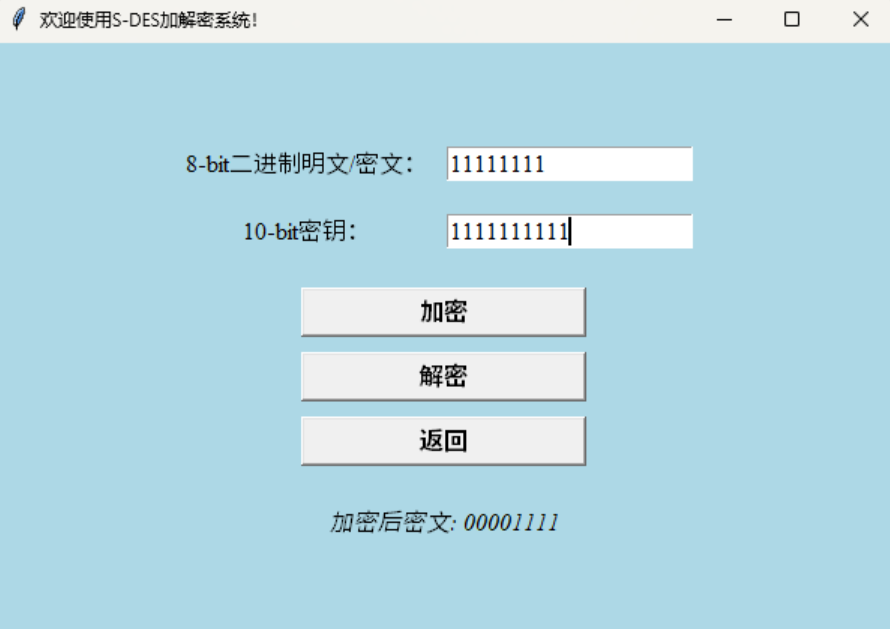
选择相同的密钥K为：1111111111

相同的明文P为：11111111

同时，**常子昕组**使用我们组的加密结果使用密钥K进行解密，解密后的明文为：。结果如下所示，说明我们所设计的算法是标准算法。



**常子昕组**测试结果：



可见同明文，同密钥最后的加密结果都为00001111，结果相同，交叉测试成功。

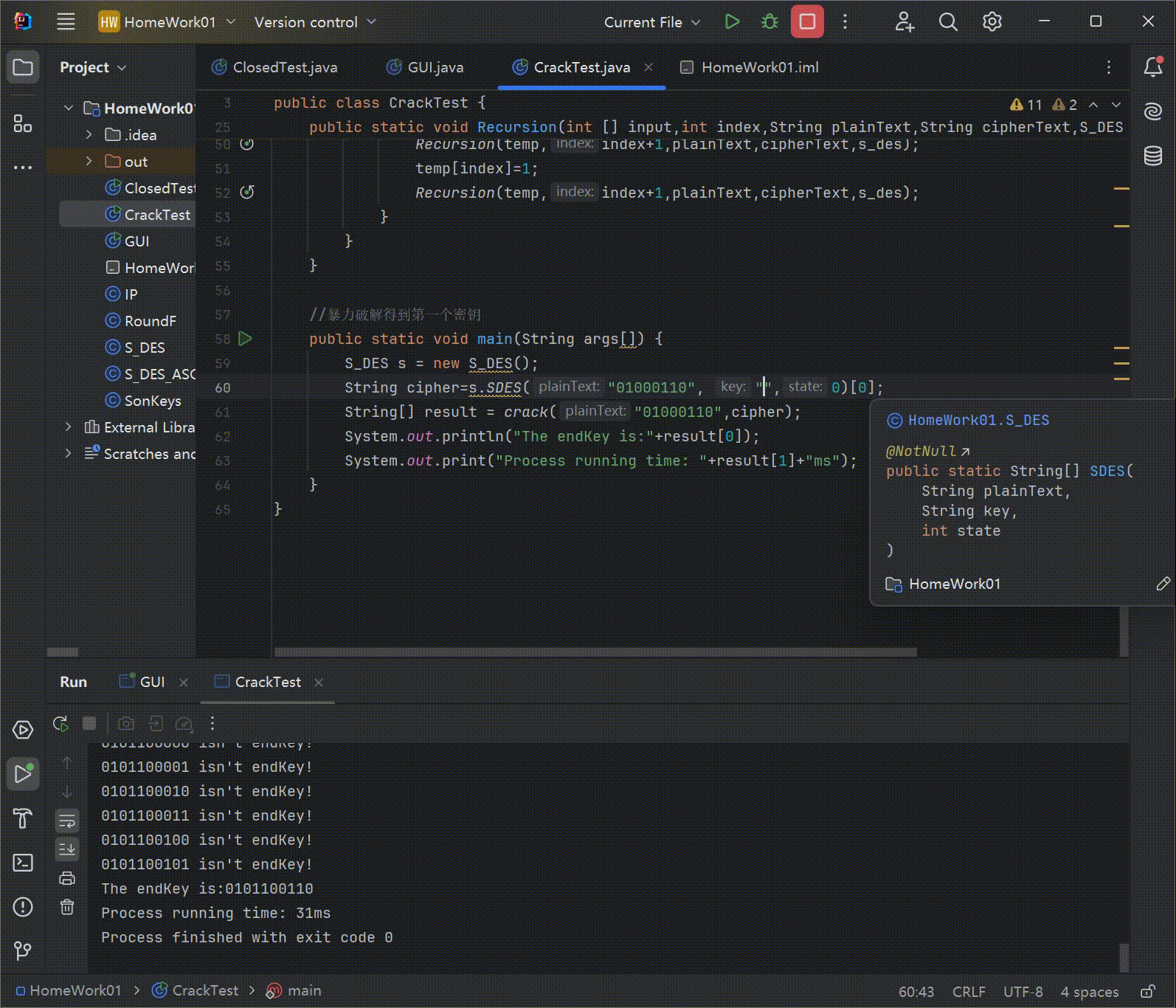
1. 扩展功能测试
   1. 实用性扩展，数据输入可以是ASII编码字符串(分组为1 Byte)，对应地输出也可以是ACII字符串(很可能是乱码)

使用密钥1011110010对字符串wmssjsjk加密并解密



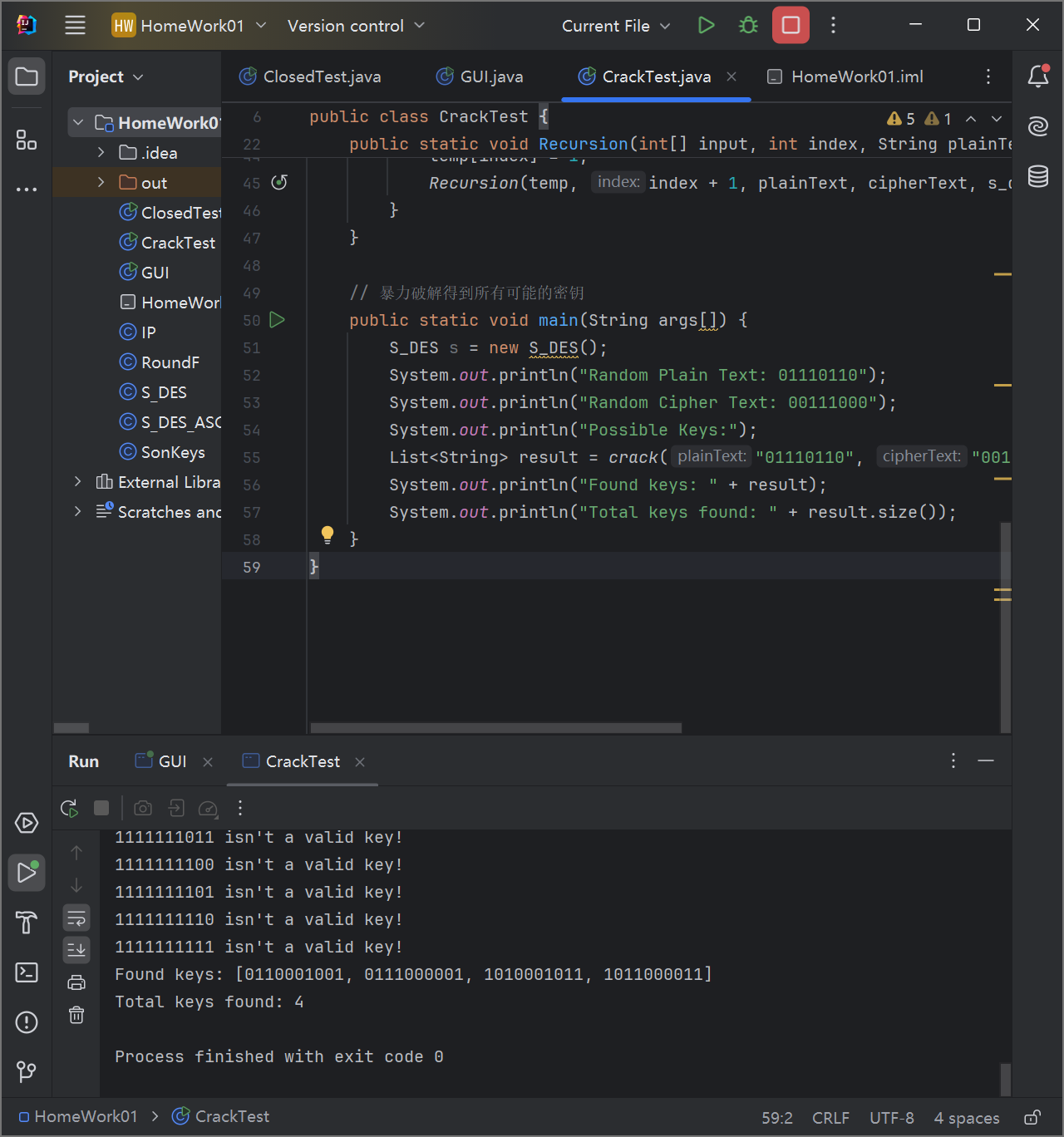
结果可见，同密钥加密得到的密文使用同密钥解密后得到的明文与最初值相同，扩展功能通过。

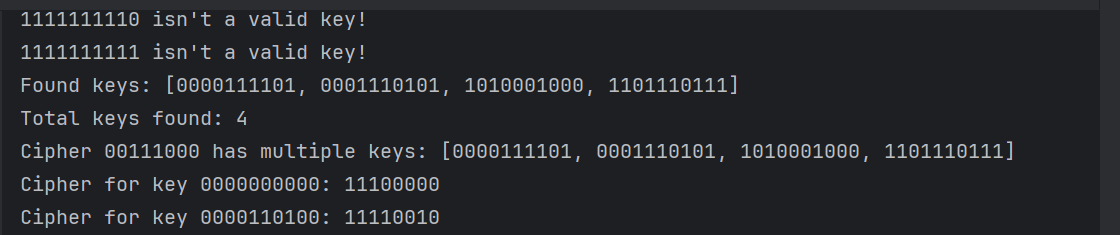
1. 暴力破解测试
   1. 破解过程：



在已知一对明文与密文的情况下，成功破解SDES算法获得第一个密钥用时为31ms。

1. 封闭测试
2. 随机选择的一个明密文对，是不是有不止一个密钥Key
3. 对应明文空间任意给定的明文分组P，是否会出现选择不同的密钥加密得到相同密文Cn的情况？





可见密文 00111000 对应多个密钥，这进一步验证了 S-DES 算法的特性，即不同的密钥可以加密相同的明文生成相同的密文。

不同密钥的加密结果：

对于密钥 0000000000，加密明文 11101110 得到的密文是 11100000。

对于密钥 0000110100，加密同样的明文得到的密文是 11110010。

这表明不同的密钥确实可以产生不同的密文，且在此例中，两个不同的密钥加密相同的明文得到了不同的结果。

结论

在 S-DES 加密中，存在多个密钥可以加密相同的明文生成相同的密文，这可能会影响加密的安全性。

不同的密钥可以产生不同的密文，这表明 S-DES 算法在密钥选择上具有一定的灵活性和复杂性。