S-DES测试结果

**第1关：基本测试**

**测试目标：**验证S-DES算法程序是否能够正确加密和解密8位的数据。

**测试结果：**经过测试，S-DES算法程序能够正确加密和解密8位的数据，并产生准确的密文。

测试步骤和结果：  
（1）加密：

明文：10011100

密钥：1011011000

密文：11100011

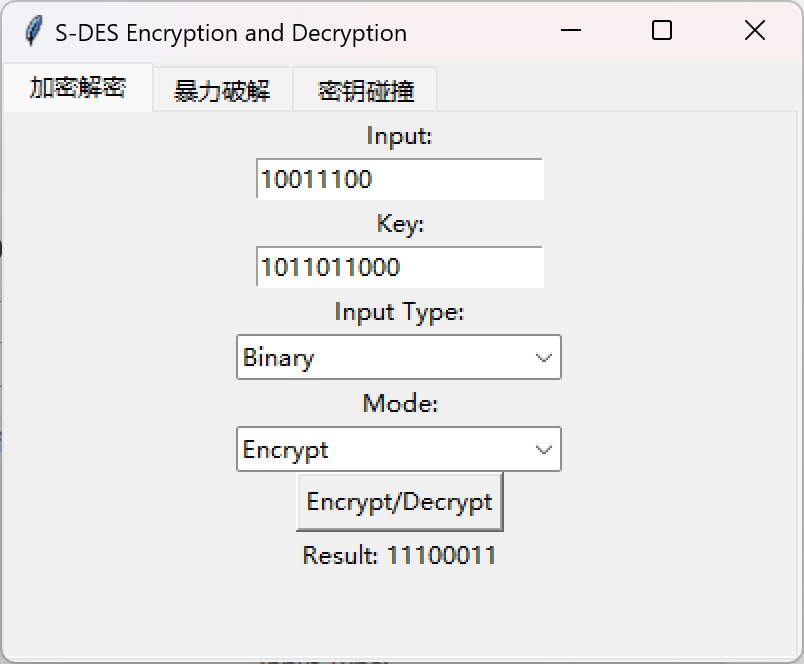


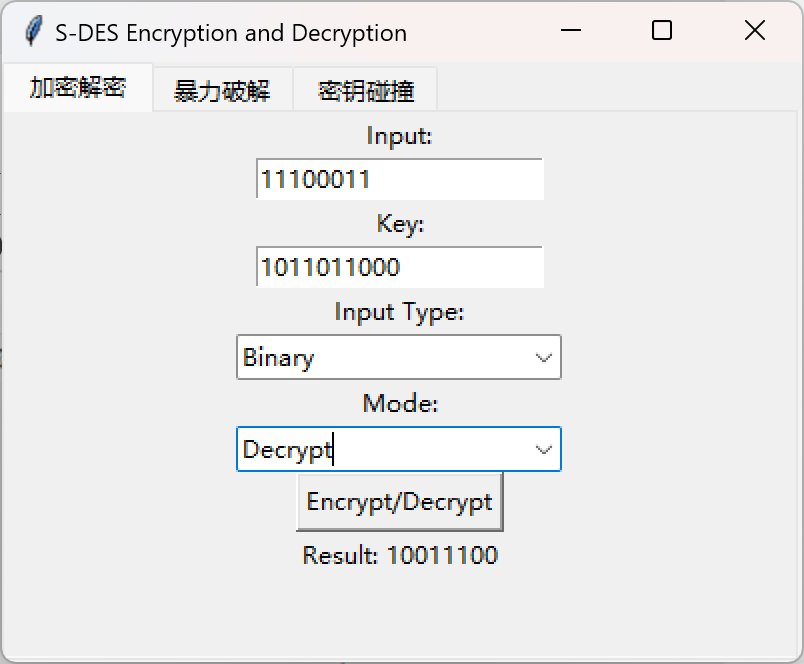
图1.1

（2）解密：

密文：11100011

密钥：1011011000

明文：10011100



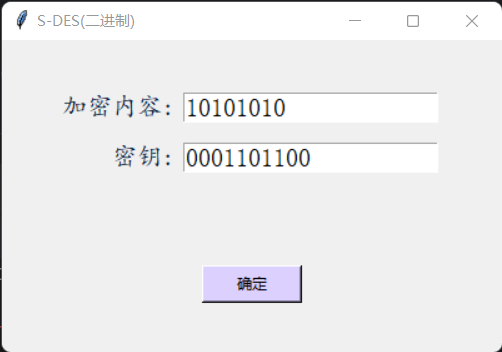
**第2关：交叉测试**

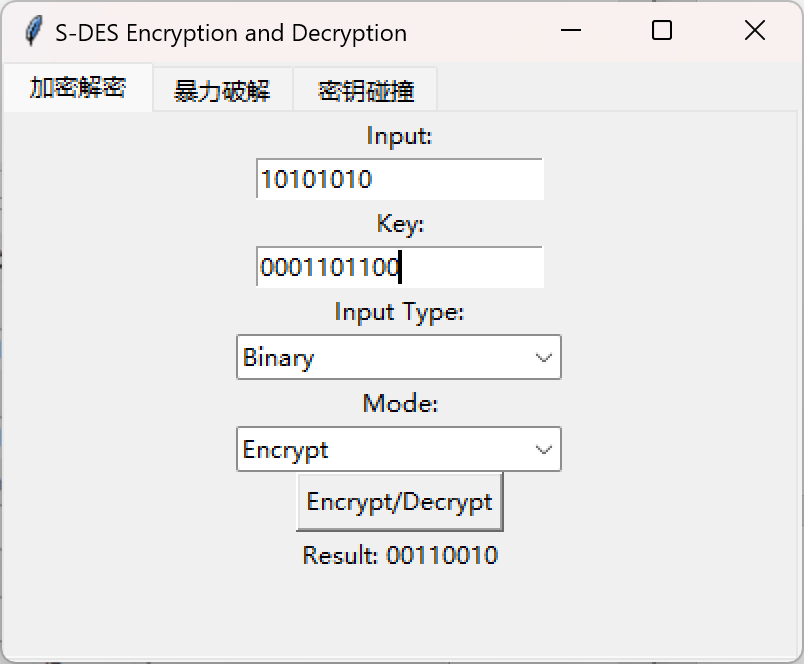
**测试目标：**验证不同人员编写的S-DES算法程序使用相同的密钥和明文时，能够得到相同的密文。

**测试结果：**经过交叉测试，不同编写的S-DES算法程序能够使用相同的密钥和明文得到相同的密文。

测试步骤和结果：

|  |  |  |
| --- | --- | --- |
| **测试输入** | **程序A输出** | **程序B输出** |
| 明文：10101010  密钥：0001101100 | 密文：00110010 | 密文：00110010 |

程序A：  


程序B（当前）：  


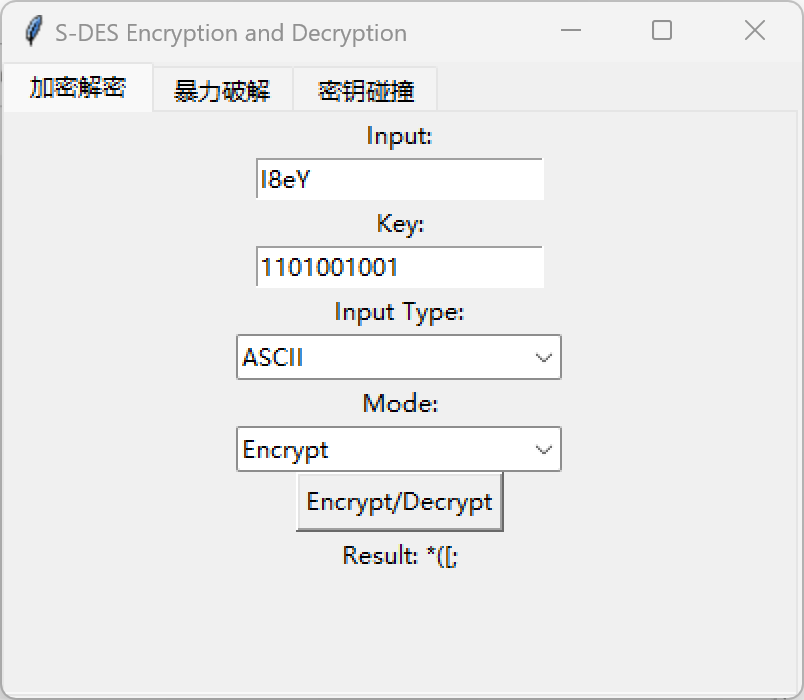
**第3关：扩展功能**

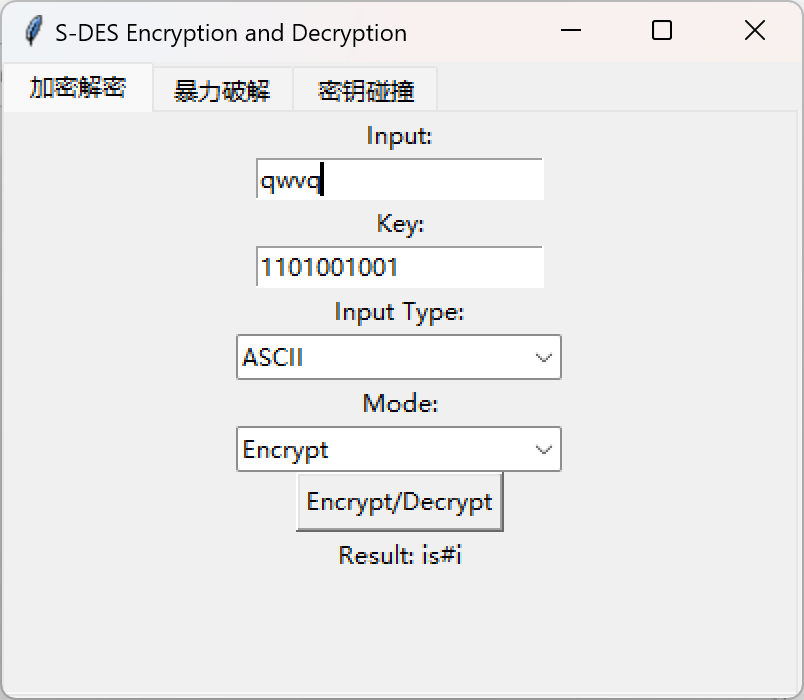
**测试目标：**验证S-DES算法程序是否能够处理ASCII编码字符串的加密和解密。

**测试结果：**经过测试，S-DES算法程序能够处理ASCII编码字符串的加密和解密，并产生相应的ASCII编码的密文。

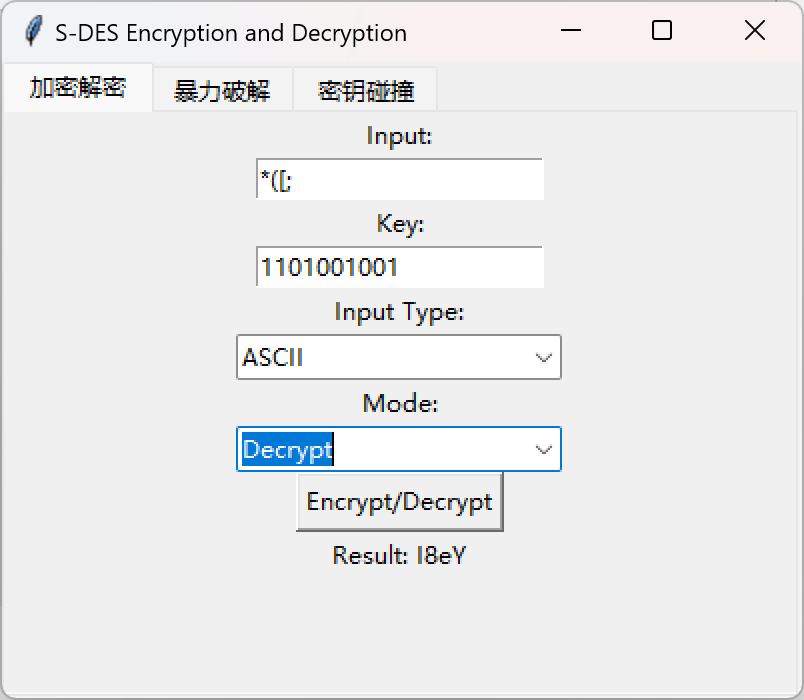
测试步骤和结果：  
（1）加密

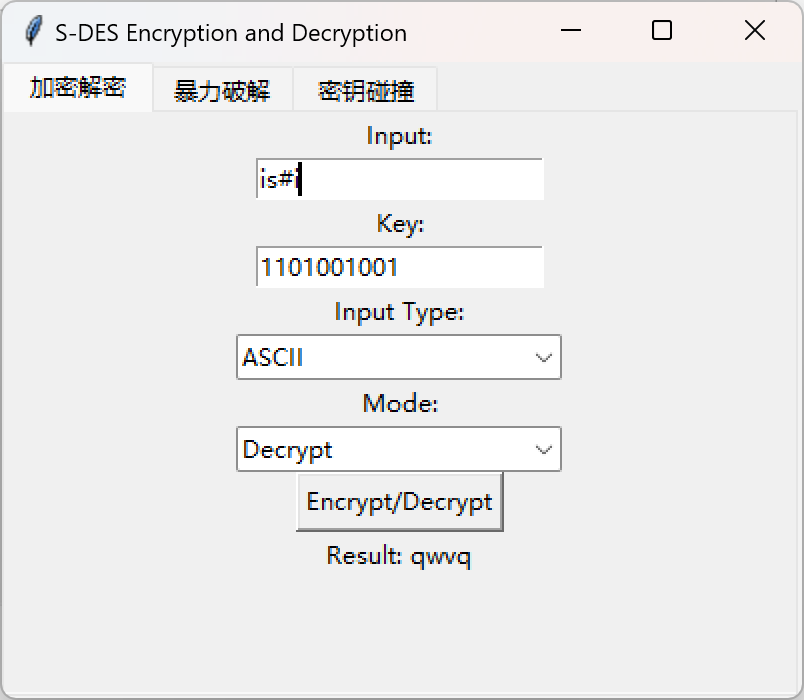
|  |  |
| --- | --- |
| **测试输入** | **输出** |
| 明文：I8eY 密钥：1101001001 | 密文：\*([; |
| 明文：qwvq 密钥：1101001001 | 密文：is#i |



  
（2）解密

|  |  |
| --- | --- |
| **测试输入** | **输出** |
| 密文：\*([; 密钥：1101001001 | 明文：I8eY |
| 密文：is#i 密钥：1101001001 | 明文：qwvq |





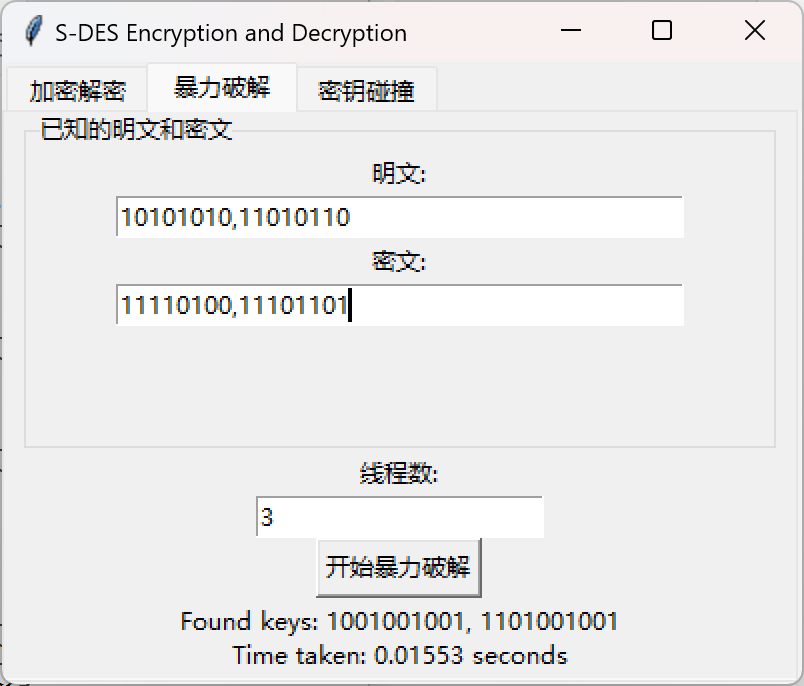
**第4关：暴力破解**

**测试目标：**验证S-DES算法程序能否使用暴力破解方法找到正确的密钥。

**测试结果：**经过暴力破解测试，S-DES算法程序能够成功找到使用相同密钥的明文和密文对，并找到正确的密钥。

测试步骤和结果：

|  |  |  |
| --- | --- | --- |
| **已知明文** | **已知密文** | **破解结果** |
| 10101010,11010110 | 11110100,11101101 | 密钥：1001001001, 1101001001 |
| 11111111 | 10111010 | 密钥：1010000000,  1110000000 |



  
另附视频在文件夹中，名字为“暴力破解”。

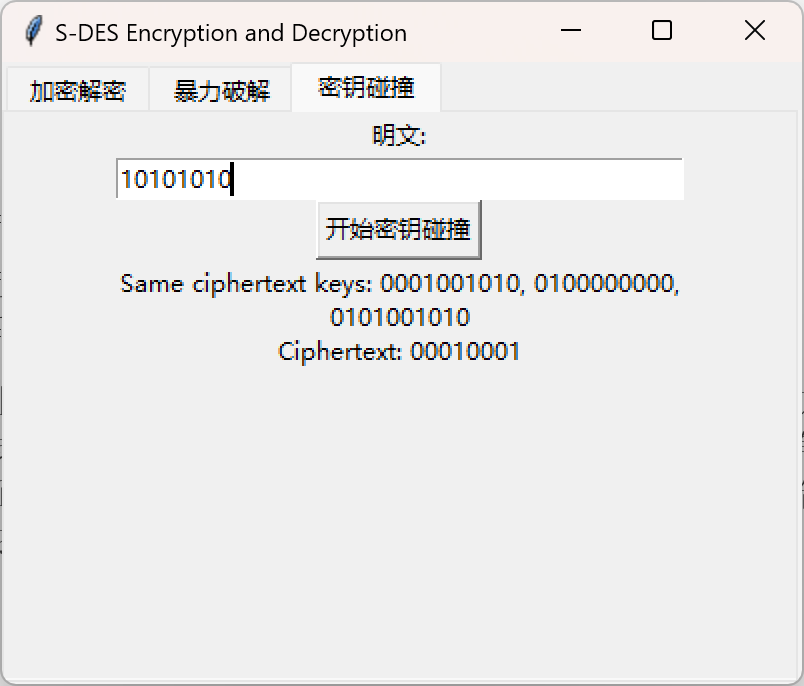
**第5关：封闭测试**

**测试目标：A**验证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；B对于随机选择的一个明密文对，是不是有不止一个密钥。

**测试结果：**经过封闭测试，S-DES算法程序中对应明文空间任意给定的明文分组P\_{n}，会出现选择不同的密钥，加密得到相同密文的情况。对于随机选择的一个明密文对，不止一个密钥。

测试步骤和结果：  
A：

|  |  |  |
| --- | --- | --- |
| **明文** | **不同密钥** | **相同密文** |
| 10101010 | 0001001010,0100000000,0101001010 | 00010001 |



B:

|  |  |
| --- | --- |
| **一组明密文** | **密钥** |
| 明文：00000000 密文：11111111 | 0001000100, 0101000100 |

