TiMi 小组关于 S-DES 加解密项目开发手册

一．概述

本项目可通过 GUI 界面实现对二进制、ASCII 编码的数据进行加/解密，同时还可通过暴力破解获得多对明密文对相应的密钥以及一对明密文对可能存在的多个密钥。

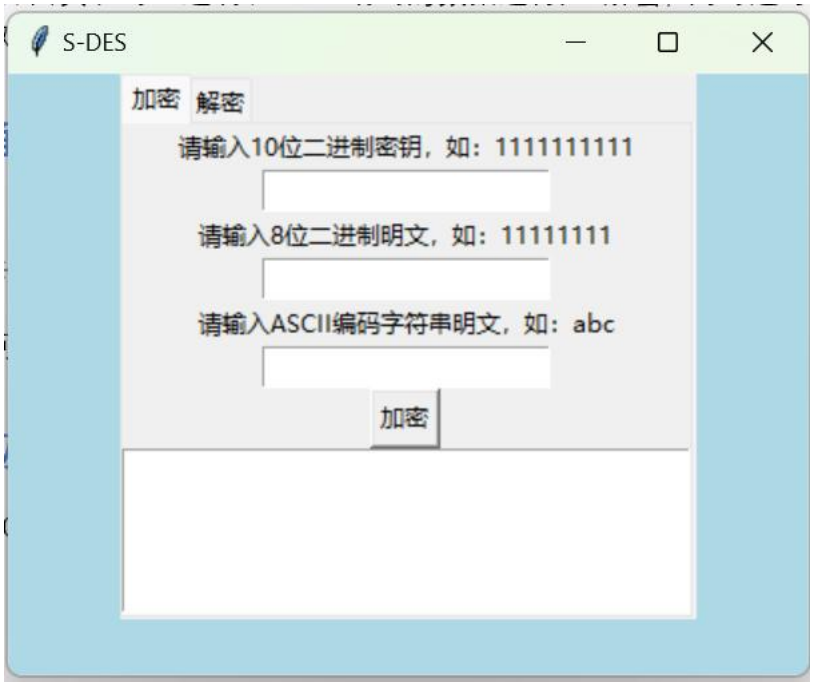
二．GUI 界面

2.1 相关代码

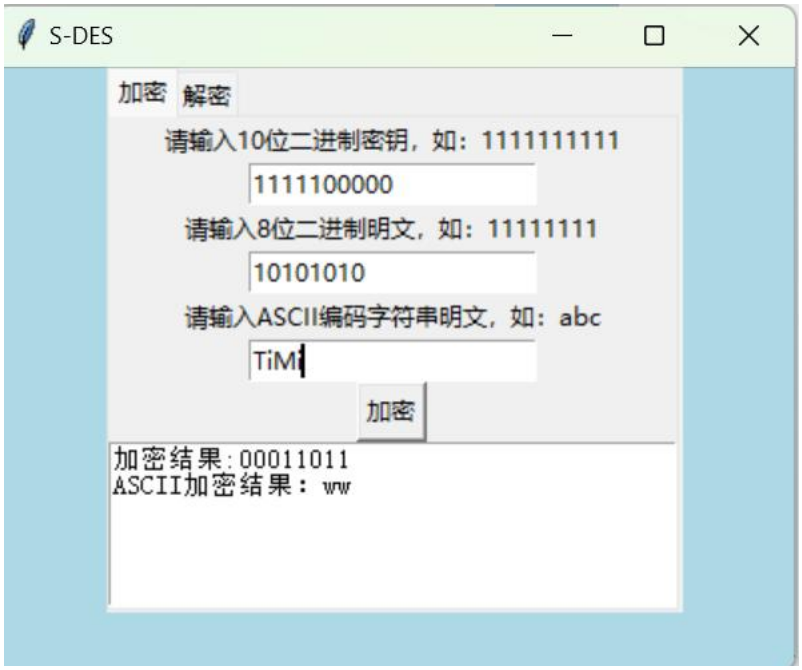
GUI 界面相关代码可参考代码项目中 GUI.py 相关文件。

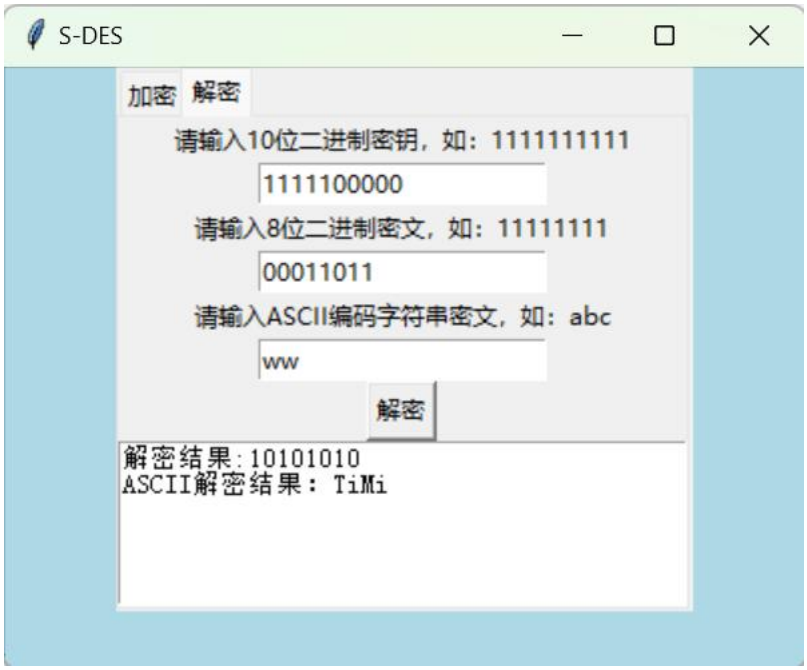
2.2 具体界面及操作解释

用户可以通过运行 GUI.py 文件可得：

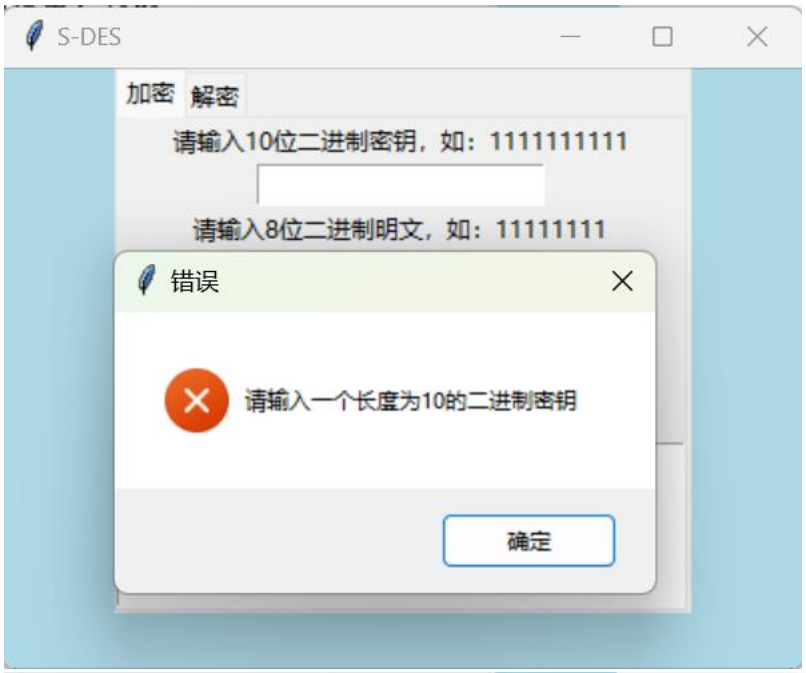


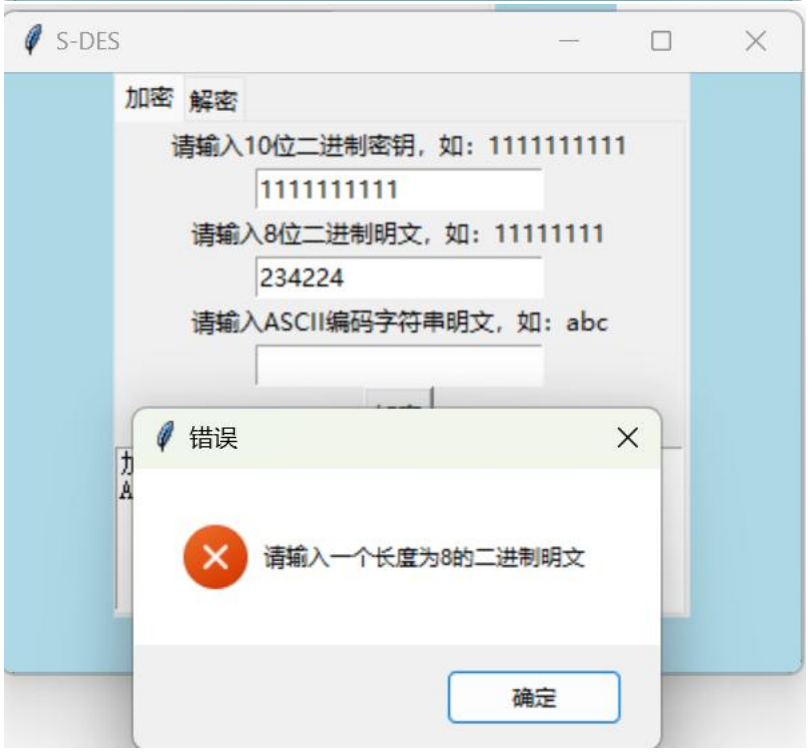
用户输入密钥以及明/密文，可进行加/解密：

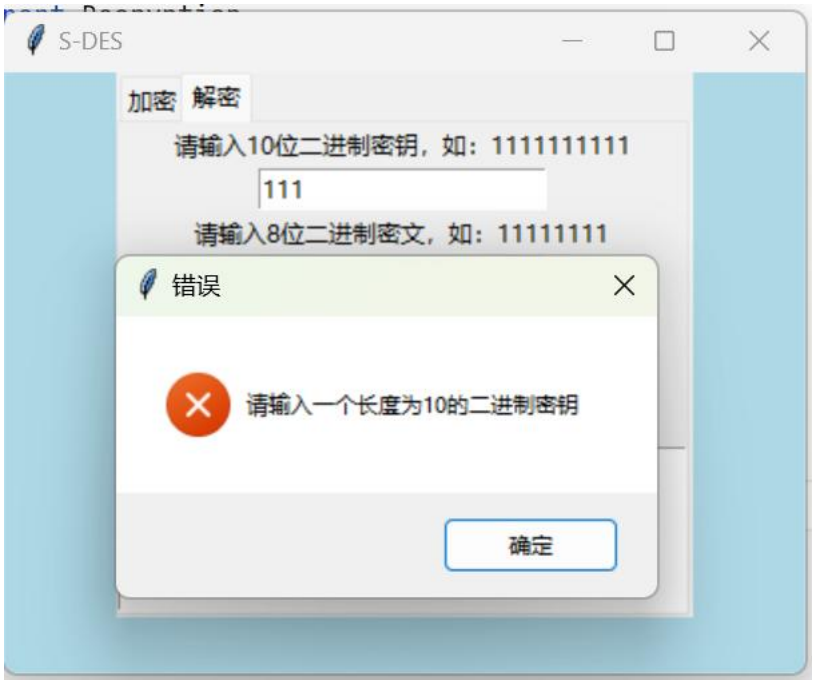


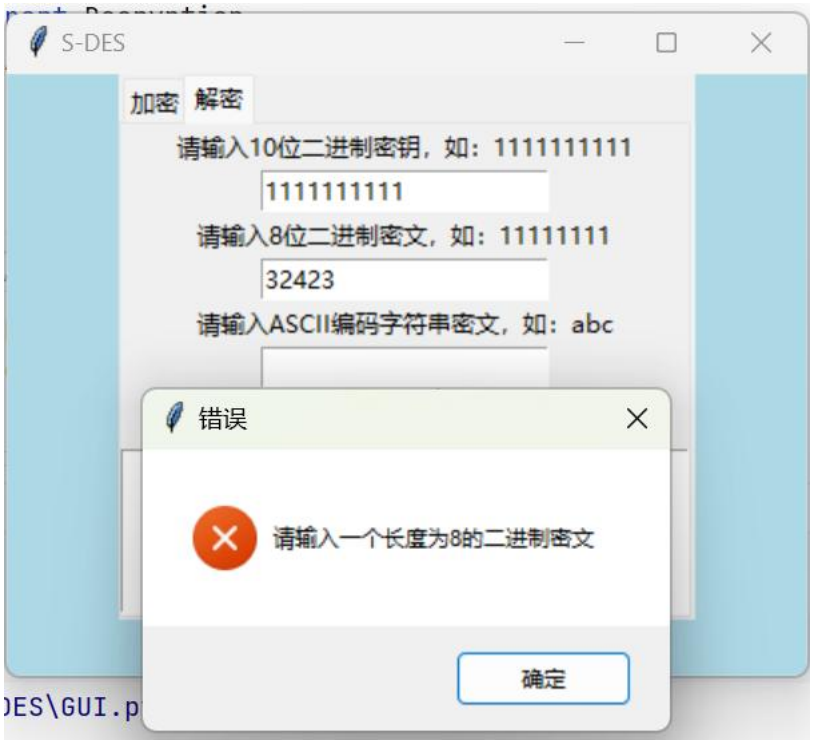


若输入密钥或者明文的长度、格式不对（比如密钥长度不为 10，二进制明文长度不为 8，或者格式不为二进制），会有相关提醒：


S-DES
加密
解密
请输入10位二进制密钥，如：1111111111
请输入8位二进制明文，如：11111111
错误
请输入一个长度为10的二进制密钥
确定


S-DES
加密
解密
请输入10位二进制密钥，如：1111111111
1111111111
请输入8位二进制明文，如：11111111
234224
请输入ASCII编码字符串明文，如：abc
错误
请输入一个长度为8的二进制明文
确定





暴力破解：

```
D:\python\python.exe "D:\imformation safety\S-DES\BF.py"
请输入明密文对对数：2
请输入第1对8-bit明文：10001111
请输入第1对8-bit密文：10010000
请输入第2对8-bit明文：11100100
请输入第2对8-bit密文：11000111
```

```
第 85次：密钥为0001010100，密文为11000001，未匹配！
第 86次：密钥为0001010101，密文为00001000，未匹配！
第 87次：密钥为0001010110，密文为00110001，未匹配！
第 88次：密钥为0001010111，密文为01011100，未匹配！
成功破解密钥为 0001011000
尝试次数： 89
破解时间： 0.003022432327270508 秒


第1对明密文对找到密钥：0001011101  尝试次数：93,破解时间：0.0020110607147216797秒
第2对明密文对找到密钥：0001011000  尝试次数：88,破解时间：0.003022432327270508秒
2对明密文暴力破解找到密钥的平均用时为：0.0025167465209960938秒
```

```
D:\python\python.exe "D:\imformation safety\S-DES\BF2.py"
请输入8-bit明文：10101010
请输入8-bit密文：00011011
找到密钥1:1000011001  累计尝试次数： 538，累计破解时间： 0.011337995529174805 秒
找到密钥2:1011100000  累计尝试次数： 737，累计破解时间： 0.014404296875 秒
找到密钥3:1100011001  累计尝试次数： 794，累计破解时间： 0.015425443649291992 秒
找到密钥4:1111100000  累计尝试次数： 993，累计破解时间： 0.019562959671020508 秒

进程已结束,退出代码0
```

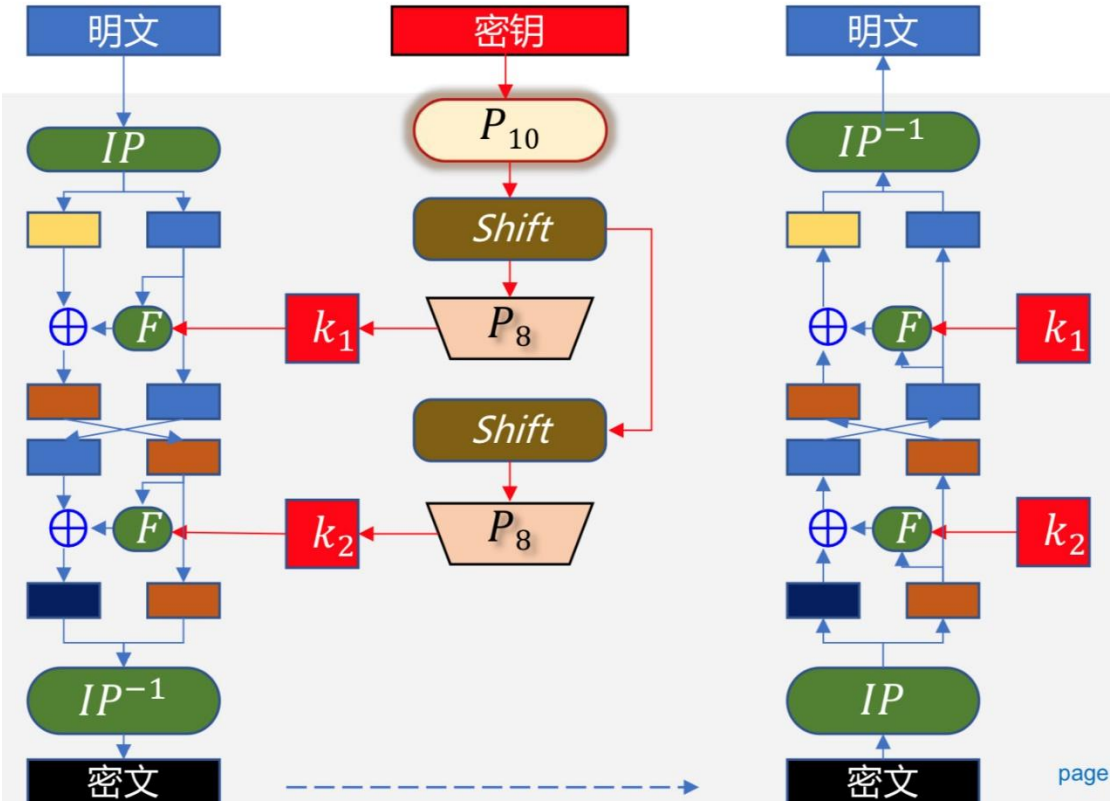
三．项目代码部分相关介绍

其中 GUI.py 主要关于界面的设计；Function.py 主要设计 EP-Box，S-Box，SP-Box，IP，IP 的逆，轮函数的设计；Key.py 主要设计了提取子密钥；Encryption.py 主要完成加密过程；Decryption.py 主要完成解密过程；ASCII.py 完成了对于 ASCII 编码的加/解密；BF.py 完成了多对明密文的密钥破解；BF2.py 完成了破解一对明密文可能存在的多个不同密钥。

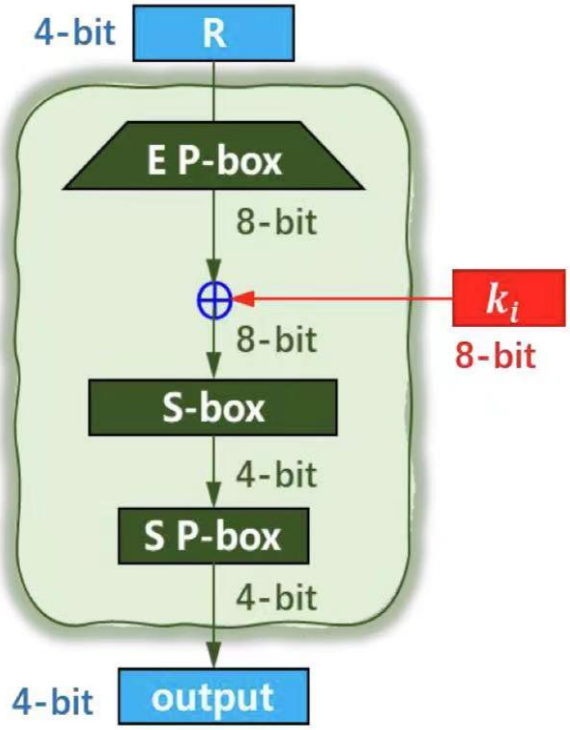
可运行文件为：GUI.py；BF.py；BF2.py

四．项目背景介绍

S-DES 算法加/解密原理流程图如下：



轮函数原理流程如下：



五．使用步骤

●运行 GUI.py 文件

●可选择“加密”或者“解密”选项

●输入相应的密钥，二进制明/密文（可选），ASCII 编码的明/密文（可选），选择加/解密

●若进行暴力破解，可运行 BF.py 文件或者时 BF2.py 文件

六．其他帮助

TiMi 小组是一个优秀、热情负责的团队。若您在使用过程中出现任何困惑不解，可发送邮件至 891073279@qq.com 或者 3416924346@qq.com。