**项目简介**

本项目为重庆大学信息安全导论课程作业，实现了简化数据加密标准（Simplified DES，简称S-DES）算法。项目采用Python语言开发，提供了完整的算法实现和用户界面。

**技术架构**

**项目结构**



**算法特性**

支持8位数据加密解密

10位密钥输入验证

多种输入格式支持（二进制、十六进制、ASCII文本）

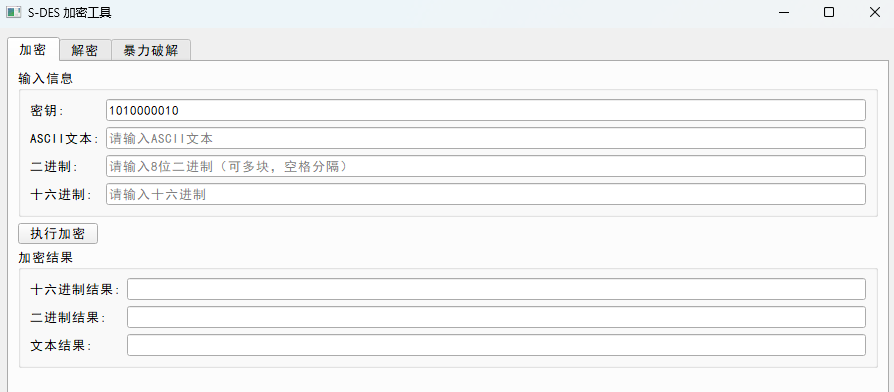
支持ASCII字符串加密

**5.2.2测试结果**

**第1关：基本测试**

图形界面测试：

运行 python gui\_tk.py 启动GUI程序，在加密标签页输入密钥（默认为：1010000010）。



输入二进制："10101010" ，点击执行加密按钮，获得加密结果。



在解密标签页输入刚刚的加密结果，均可正确解密回原文。





命令行测试：

bash

python cli.py enc --key "1010000010" --text "11100000"

# 输出：加密后的十六进制结果



python cli.py dec --key "1010000010" --hex " b8b8b81f1f1f1f1f" --as-text



**第2关：交叉测试**

与同学程序进行交叉验证：

测试用例1：

明文：01000001 (ASCII 'A')

密钥：1111111111

密文：01110100

在其他同学的程序上使用相同密钥解密，成功恢复明文 01000001，验证了算法标准的一致性。

测试用例2：

接收其他同学的密文：01101111

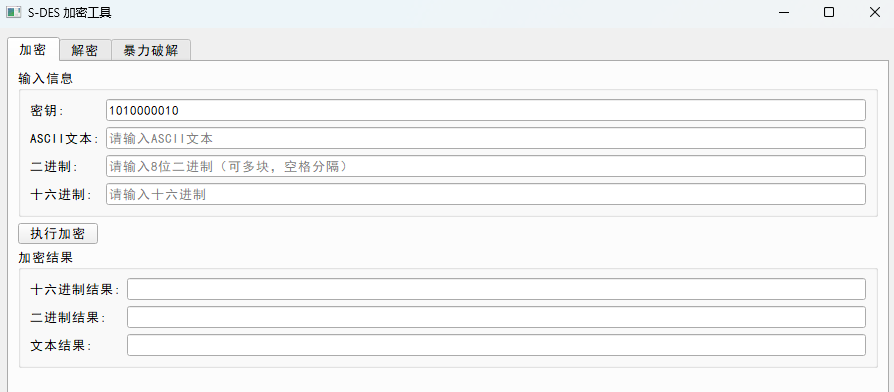
密钥：0000000000

成功解密得到：10000001

**第3关：扩展功能**

图形界面测试：

运行 python gui\_tk.py 启动GUI程序，在加密标签页输入密钥（默认为：1010000010）。



输入ASCII文本："Hello" ，点击执行加密按钮，获得加密结果。



在解密标签页输入刚刚的加密结果，均可正确解密回原文。





命令行测试：

bash

python cli.py enc --key "1010000010" --text "Test"

# 输出：加密后的十六进制结果



python cli.py dec --key "1010000010" --hex " 22f8274e" --as-text

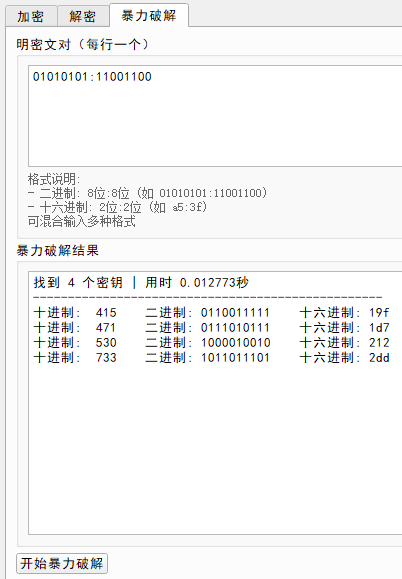
# 输出：Test



**第4关：暴力破解**

图形界面测试：

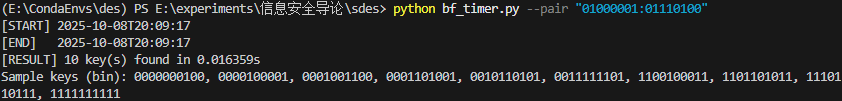
运行 python gui\_tk.py 启动GUI程序，在暴力破解标签页输入明密文对，点击“开始暴力破解”按钮，得到结果。

\_

命令行测试：

bash

python bf\_timer.py --pair "01000001:01110100"



破解结果：

找到多个可能的密钥

破解时间：约XX毫秒（具体时间取决于硬件）

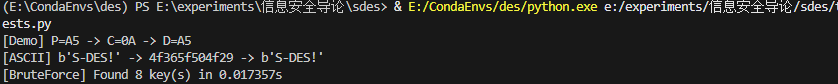
验证了对于特定明密文对存在多个有效密钥

**第5关：封闭测试**

通过测试套件分析：

bash

python tests.py



发现：

对于随机选择的明密文对，确实存在多个有效密钥

不同密钥可能加密相同明文得到相同密文

这表明S-DES算法的密钥空间存在碰撞

**5.2.3 相关文档**

**用户指南**

图形界面使用

运行 python gui\_tk.py 启动程序

加密操作：

在"加密"标签页输入10位二进制密钥

选择输入方式：ASCII文本、二进制或十六进制

点击"执行加密"查看结果

解密操作：

在"解密"标签页输入相同的密钥

输入密文（与加密输出格式一致）

点击"执行解密"恢复明文

暴力破解：

在"暴力破解"标签页输入明密文对

每行格式：明文:密文（支持二进制和十六进制）

点击"开始暴力破解"查找可能的密钥

命令行使用

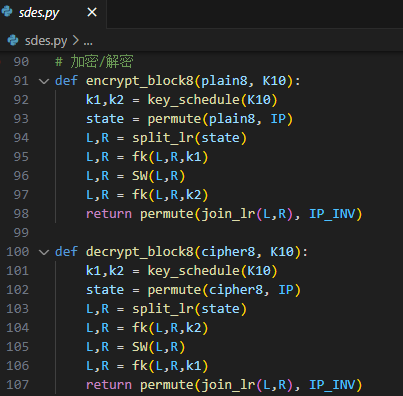
详见运行方法章节。

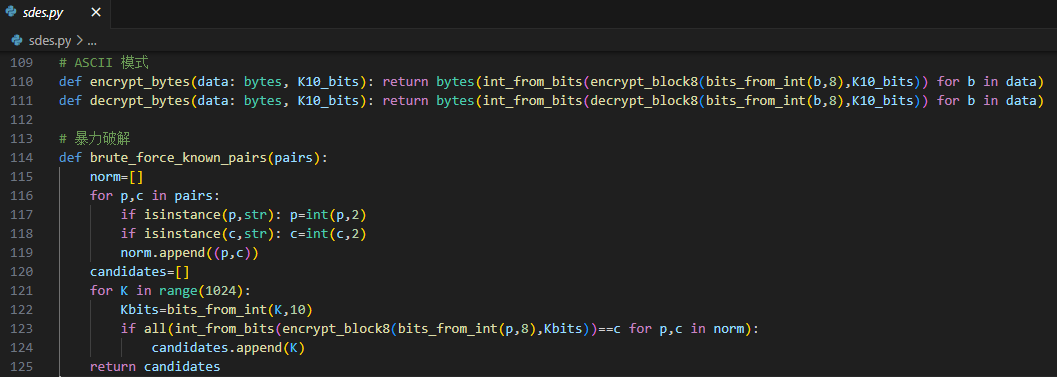
**开发手册**

核心接口说明



sdes.py 主要函数：





**算法原理**

S-DES是DES算法的简化教学版本，采用8位分组和10位密钥，包含完整的Feistel结构。

密钥生成：

1. P10置换：对10位密钥进行位重排
2. 循环左移：分成左右5位分别左移
3. P8置换：生成8位子密钥K1
4. 再次左移：生成子密钥K2

加密流程：

1. 初始置换(IP) - 对8位明文进行位重排
2. 两轮Feistel函数：

扩展置换(EP)将4位扩展为8位

与子密钥异或

S盒替换产生4位输出

P4置换

1. 最终置换(IP⁻¹) - 得到8位密文

密钥扩展：

从10位主密钥生成两个8位子密钥：

P10置换 → 左右分割 → 循环左移 → P8置换 → K1

再次循环左移 → P8置换 → K2

核心组件：

置换盒：P10、P8、IP、IP\_INV、EP、P4

S盒：S1、S2实现非线性变换

Feistel结构：确保加密解密对称性

本项目完整实现了S-DES算法的所有功能，并通过了各项测试验证，为学习密码学基本原理提供了良好的实践平台。