S-DES 加密工具开发手册

一、项目概述

S-DES（Simplified Data Encryption Standard）是一个简化的 DES 加密算法实现，使用 10 位密钥对 8 位数据进行加密。本项目提供了一个完整的图形用户界面，支持二进制和文本的加密解密操作，以及密钥分析功能。

1.主要特性

- 二进制加解密：支持 8 位和 10 位二进制数据的加密和解密
- 文本加解密：支持任意长度文本的加密和解密
- 密钥分析：提供暴力破解和密钥冲突分析功能
- 多线程支持：防止界面卡顿
- 用户友好界面：清晰的标签页设计和实时状态反馈

二、项目结构

```
SDES_Tool/
├─── DES_1.py                # S-DES 算法核心实现及图形用户界面
└─── README.md               #  项目文档
```

1.核心组件

（1） SDES 类

S-DES 算法的核心实现，包含所有加密解密逻辑。

主要方法：

generate_keys(key) - 生成子密钥

encrypt_block(plaintext, key) - 加密单个 8 位块

decrypt_block(ciphertext, key) - 解密单个 8 位块

encrypt_string(text, key) - 加密字符串

decrypt_string(cipher_text, key) - 解密密文字符串

（2）SDESGUI 类

图形用户界面实现，使用 tkinter 构建。

主要组件：

- 二进制加解密标签页
- 文本加解密标签页
- 密钥分析标签页
- 多线程处理
- 进度显示

2.设计模式

（1）单例模式

GUI 类作为应用程序的主控制器。

（2）观察者模式

通过 tkinter 的事件机制实现用户交互。
（3）工厂模式
密钥生成和置换操作使用工厂方法模式。
（4）错误处理
- 输入验证：确保二进制输入格式正确
- 异常捕获：处理加密解密过程中的异常
- 线程安全：防止多线程访问冲突

三、接口文档

1.SDES 类接口

（1）permute(bits, permutation)
功能：执行置换操作
参数：
- bits (list): 输入位列表
- permutation (list): 置换表
返回：置换后的位列表
（2）generate_keys(key)
功能：生成子密钥 k1 和 k2
参数：
- key (list): 10 位密钥
返回：元组 (k1, k2)
（3）encrypt_block(plaintext, key)
功能：加密一个 8 位分组
参数：
- plaintext (list): 8 位明文
- key (list): 10 位密钥
返回：8 位密文
（4）decrypt_block(ciphertext, key)
功能：解密一个 8 位分组
参数：
- ciphertext (list): 8 位密文
- key (list): 10 位密钥
返回：8 位明文
（5）encrypt_string(text, key)
功能：加密字符串
参数：
- text (str): 输入文本
- key (list): 10 位密钥
返回：加密后的字符串
（6）decrypt_string(cipher_text, key)
功能：解密密文字符串
参数：

- cipher_text (str): 密文
- key (list): 10 位密钥
返回：解密后的明文

2.SDESGUI 类接口
（1）create_binary_operations_tab()
功能：创建二进制操作标签页
（2）create_text_operations_tab()
功能：创建文本操作标签页
（3）create_key_analysis_tab()
功能：创建密钥分析标签页
（4）encrypt_binary()
功能：执行二进制加密
（5）decrypt_binary()
功能：执行二进制解密
（6）encrypt_text()
功能：执行文本加密
（7）decrypt_text()
功能：执行文本解密
（8）start_brute_force()
功能：开始暴力破解
（9）analyze_key_conflicts()
功能：分析密钥冲突

四、扩展指南

1. 在 SDES 类中添加新的加密方法，代码如下：
```
@staticmethod
def encrypt_mode_new(data, key, mode):
    # 实现新的加密模式
    pass
```

2. 在 GUI 中添加对应的界面元素，代码如下：
```
def create_new_mode_tab(self):
    # 创建新的标签页
    pass
```

3.可以修改以下常量来调整算法行为，代码如下：
```
# 在 SDES 类中修改这些常量
P10 = [3, 5, 2, 7, 4, 10, 1, 9, 8, 6]   # P10 置换表
P8 = [6, 3, 7, 4, 8, 5, 10, 9]          # P8 置换表
S0 = [[1, 0, 3, 2], ...]                # S 盒定义
```