S-DES 加密算法工具用户指南

简介：

S-DES 加密算法工具是一款基于简化数据加密标准 (Simplified Data Encryption Standard) 的加密解密工具，提供基础加解密、字符串处理、密钥暴力破解和算法分析等功能。本工具界面友好，操作简单，适合学习和研究对称加密算法的基本原理。

安装与启动：

确保您的系统已安装 Python 3.x 环境

将所有程序文件（main.py, gui.py, sdes\_core.py, ascii\_processor.py, brute\_force.py, closed\_test.py）放在同一目录下

运行 main.py 启动程序

功能说明

程序包含四个主要功能模块，通过顶部标签页进行切换：

### 1. 基础加解密

该模块用于对 8 位二进制数据进行加密和解密操作。

使用步骤：

在 "8 位输入 (二进制)" 框中输入 8 位二进制数（仅包含 0 和 1）

在 "10 位密钥 (二进制)" 框中输入 10 位二进制密钥

点击 "加密" 按钮将明文转换为密文，或点击 "解密" 按钮将密文转换为明文

结果将显示在 "输出结果" 框中

注意事项：

输入必须严格遵守长度要求（8 位数据，10 位密钥）

输入只能包含 '0' 和 '1' 字符

2. 字符串处理

该模块用于对 ASCII 字符串进行加密和解密，内部会自动将字符串转换为二进制后进行处理。

使用步骤：

在 "输入文本" 框中输入要处理的 ASCII 字符串

在 "10 位密钥 (二进制)" 框中输入 10 位二进制密钥

点击 "加密字符串" 按钮将明文转换为密文，或点击 "解密字符串" 按钮将密文转换为明文

结果将显示在 "输出结果" 框中

注意事项：

密钥必须是 10 位二进制数

加密后的字符串可能包含不可打印字符

### 3. 密钥暴力破解

该模块可通过已知明文和对应密文，遍历所有可能的密钥（共 1024 种）来找到正确的密钥。

使用步骤：

选择破解模式：

二进制模式：用于破解 8 位二进制数据的密钥

ASCII 模式：用于破解字符串的密钥

根据所选模式输入相应的明文和密文：

二进制模式：输入 8 位二进制明文和对应的 8 位二进制密文

ASCII 模式：输入 ASCII 明文字符串和对应的加密字符串（长度必须相同）

点击 "开始暴力破解" 按钮

破解进度将通过进度条显示，结果将显示在下方结果区域

注意事项：

破解过程通常只需几秒钟

可能找到多个可能的密钥（密钥碰撞现象）

结果区域会显示所有可能的密钥及其验证结果

4. 算法分析

该模块用于分析 S-DES 算法的特性，主要检测密钥碰撞现象（即不同密钥对同一明文加密得到相同密文）。

使用步骤：

点击 "开始算法分析" 按钮

分析进度将通过进度条显示

分析完成后，结果区域将显示：

总处理时间和测试参数

密钥碰撞统计数据

最大碰撞情况详情

算法安全性评估

注意事项：

分析过程会遍历所有 1024 个可能的密钥，可能需要几秒钟时间

分析结果将展示 S-DES 算法的理论特性和实际表现的对比

### 常见问题

为什么会找到多个密钥？

由于 S-DES 的密钥空间 (1024) 大于密文空间 (256)，根据鸽巢原理，必然存在密钥碰撞现象，即不同密钥可能产生相同的加密结果。

加密后的字符串显示乱码？

正常现象，因为加密后的二进制数据转换为 ASCII 字符时，可能对应不可打印字符。

程序无响应？

进行暴力破解或算法分析时，程序正在后台处理，请等待进度条完成。

若长时间无响应，可关闭程序重新启动。

输入验证失败？

请检查输入是否符合要求：二进制必须是 0 和 1 的组合，且长度正确。

### 技术说明

本工具实现的 S-DES 算法遵循以下规范：

10 位密钥，生成两个 8 位子密钥

8 位数据块加密

包含初始置换、Feistel 网络、S 盒替换、最终置换等标准步骤

加密和解密使用相同的密钥，仅子密钥使用顺序相反