# S-DES 加密解密工具 - 用户说明

## 一、工具概述

S-DES（简化 DES）加密解密工具是一款基于图形化界面的轻量工具，支持 8 位二进制数据、ASCII 字符串的加密 / 解密，同时提供密钥暴力破解、算法封闭性测试功能，适用于密码学学习与基础数据加密场景。

## 二、系统要求

|  |  |
| --- | --- |
| 类别 | 要求 |
| 操作系统 | Windows 10/11、macOS 10.15+、Linux（Ubuntu 18.04+） |
| Python 版本 | 3.6 及以上 |
| 依赖库 | tkinter（Python 默认自带，无需额外安装） |

## 三、安装与启动

### 1. 安装步骤

无需复杂安装，仅需：

1. 确认设备已安装符合要求的 Python 环境（可通过python --version命令检查）；
2. 获取工具源代码文件（命名为ex1-S-DES.py）。

### 2. 启动方法

打开终端 / 命令提示符，进入源代码所在文件夹，执行命令：

|  |
| --- |
| python ex1-S-DES.py |

执行后将自动弹出工具图形界面。

## 四、界面介绍（主界面分区）

|  |  |  |
| --- | --- | --- |
| 区域 | 包含元素 | 功能说明 |
| 顶部 - 密钥区 | 密钥输入框、“默认密钥” 按钮 | 输入 10 位二进制密钥，点击 “默认密钥” 可快速填充示例密钥（1010000010） |
| 中部 - 数据区 | 明文 / 密文输入框、功能按钮（加密 / 解密 / 暴力破解 / 封闭性测试） | 输入待处理数据，点击对应按钮执行操作 |
| 底部 - 结果区 | 输出文本框、进度条 | 显示操作结果（如密文、破解密钥），进度条在暴力破解时显示进度 |

## 五、使用教程（分场景）

### 场景 1：基本二进制数据加密 / 解密

#### 加密步骤：

1. 在 “密钥输入框” 输入 10 位二进制数（如1010000010）；
2. 在 “明文 / 密文输入框” 输入 8 位二进制数（如00000000）；
3. 点击 “加密” 按钮，底部输出框将显示加密后的密文（示例：11110100）。

#### 解密步骤：

1. 保持密钥不变（需与加密时一致）；
2. 在输入框粘贴加密得到的密文（如11110100）；
3. 点击 “解密” 按钮，输出框将显示恢复的原始明文（示例：00000000）。

### 场景 2：ASCII 字符串加密 / 解密

#### 加密步骤：

1. 输入 10 位二进制密钥；
2. 在输入框直接输入 ASCII 字符串（如Hello）；
3. 点击 “加密” 按钮，输出框显示二进制格式的密文（按 8 位分组，空格分隔）。

#### 解密步骤：

1. 保持密钥与加密时一致；
2. 在输入框粘贴加密得到的二进制密文；
3. 点击 “解密” 按钮，输出框显示恢复的 ASCII 字符串（如Hello）。

### 场景 3：暴力破解密钥

#### 前提：已知 “明文 - 密文对”（如明文00000000对应密文11110100）

#### 步骤：

1. 在输入框输入已知明文（如00000000）；
2. 确保输出框已显示对应的已知密文（若未显示，可先通过正确密钥加密获取）；
3. 点击 “暴力破解” 按钮，进度条开始滚动；
4. 破解完成后，输出框显示 “找到匹配密钥：XXX”（示例：1010000010）。

### 场景 4：封闭性测试

#### 目的：检测是否存在不同密钥生成相同密文的 “密钥碰撞” 情况

#### 步骤：

1. 无需输入密钥和数据；
2. 直接点击 “封闭性测试” 按钮；
3. 系统自动生成随机明文和密钥，测试完成后输出框显示测试结论（如 “未发现密钥碰撞，算法封闭性良好”）。

## 六、输入输出格式规范

|  |  |  |
| --- | --- | --- |
| 类型 | 输入格式要求 | 输出格式说明 |
| 密钥 | 必须为 10 位二进制字符串（仅含 0 和 1） | 无输出，仅作为操作参数 |
| 二进制数据 | 8 位二进制字符串（加密 / 解密时） | 8 位一组，空格分隔（如11110100 00110011） |
| ASCII 字符串 | 任意可打印字符（如字母、数字、符号） | 直接显示可读字符；非可打印字符显示为[二进制值]（如[00001010]） |

## 七、常见问题与解决方法

|  |  |  |
| --- | --- | --- |
| 常见问题 | 原因分析 | 解决方法 |
| 点击按钮无反应 | 输入格式错误（如密钥不是 10 位二进制） | 检查输入内容，确保符合格式规范 |
| 解密结果与原明文不一致 | 解密密钥与加密密钥不匹配 | 确认解密时使用的密钥与加密时完全相同 |
| 暴力破解进度条卡住 | 程序未响应（极少发生） | 关闭工具重新启动，重新执行破解操作 |
| ASCII 解密显示乱码 | 密文格式错误或密钥错误 | 检查密文是否为加密生成的二进制串，确认密钥正确 |