S-DES 加密算法工具 用户指南

一、程序简介

本程序是基于 Python 实现的 S-DES(Simplified Data Encryption Standard)加密算法学习与演示工具。通过图形化界面,用户可以方便地进行二进制加密解密、文本加解密、密钥暴力破解及密钥冲突分析等操作。程序适用于密码学课程教学、算法演示及实验分析场景。

二、运行环境与启动方式

- 1. Python 版本: Python 3.10
- 2. 依赖库: tkinter、threading、time、itertools(均为标准库)
- 3. 启动方式:在命令行中运行 python DES_1.py,程序启动后,将显示带有多个功能选项卡的图形化界面。

三、界面结构与主要功能

程序界面主要分为三个标签页:

1. 二进制加解密; 2. 文本加解密; 3. 密钥分析



图 1 用户交互界面

四、功能模块使用方法

(一) 二进制加解密

在"二进制加解密"标签页中,用户可以输入8位二进制明文与10位二进制密钥进行加密或解密。

操作步骤:

- 1. 输入8位明文(例如 10101010);
- 2. 输入10位密钥(例如1010000010)
- 3. 点击"加密"或"解密"按钮查看结果
- 4. 可点击"示例数据"按钮快速填入测试样例

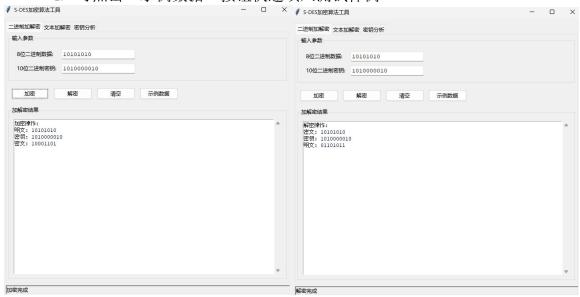


图 2 二进制加解密界面

(二) 文本加解密

在"文本加解密"标签页中,用户可以输入任意文本并使用 10 位二进制密 钥进行 S-DES 加密或解密。

操作步骤:

- 1. 输入待加密或解密的文本内容
- 2. 输入10位二进制密钥
- 3. 点击"加密文本"或"解密文本"按钮查看结果
- 4. 结果包括原文、密钥、加密结果及其十六进制表示

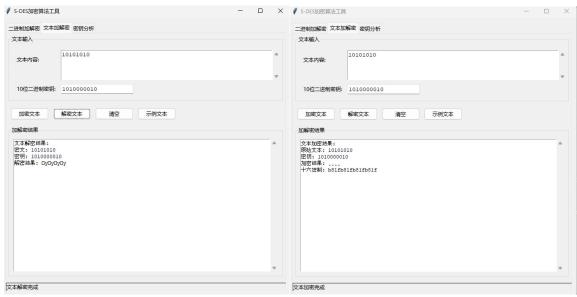


图 3 文本加解密界面

(三)密钥分析

"密钥分析"模块提供两种功能:暴力破解与密钥冲突分析。用户可通过输入已知明文和密文来模拟暴力破解,或进行多组测试分析密钥冲突。

操作步骤:

- 1. 在"已知明文"和"已知密文"中输入8位二进制数据
- 2. 点击"开始暴力破解",程序遍历所有1024个密钥(210)进行尝试
- 3. 可实时查看进度条与已找到的匹配密钥
- 4. 可点击"停止破解"中断进程
- 5. "密钥冲突分析"功能会测试多个明密文对,统计产生相同密文的不同密钥数量



S-DES加密算法工具				
进制加解密 文本加	口解密 密钥分析			
暴力破解				
已知明文:	10101010			
已知密文:	11000010			
D/442				
开始暴力破解	停止破解 示例数据			
密钥冲突分析				
ווינגגדינוויב				
	分析密钥冲突			
分析结果				
可们有未				
密文: 10001101 替代密钥数量: 3	,原密钥: 1010000010			^
测试用例 1: 明文: 10101010 密文: 10001101 替代密钥数量: 3 前5个替代密钥: 测试用例 2: 明试:11001100 密文: 11111100 替代密钥数量: 5	,原密钥: 1010000010 ['1010010110', '1011001010', '1011011110'] ,原密钥: 1110001110	1000	110']	^
测试用例 1: 明文: 10101010 密文: 10001101 替代密钥数量: 3 前5个替代密钥: 测试用例 2: 明文: 11001100 密文: 11111100 替价密钥数密: 测试用例 3: 明密: 00110011 昭文: 11110111 替代密钥数量: 3	,原密钥: 1010000010 ['1010010110', '1011001010', '1011011110'] ,原密钥: 1110001110 ['0100100011', '0100110111', '0101101011', '0101111111', '111 ,原密钥: 1100110011	1000:	110']	•
测试用例 1: 明空文: 10001101 图它文: 10001101 替代密钥数 :	,原密钥: 1010000010 ['1010010110', '1011001010', '1011011110'] ,原密钥: 1110001110 ['0100100011', '0100110111', '0101101011', '0101111111', '1111' ,原密钥: 1100110011 ['0001101110', '0001111011', '1101111011'] ,原密钥: 1010101010	1000:	110']	
测试用例 1: 则识:101010100 密文:10001101 替代密钥数量:3 前5个替代密钥: 则试:11001100 密文:11111100 替前5个替代密钥: 则试:1110110011011101111时,111101111时,11110111时,11110000。 密文:11110111时,11110000。 图文:1111001011时,11110000。 图文:111100101时,11110000。 图文:01111001时,11110000。 图文:01111001时,11110000时,11110000时,11110000时,11110000时,11110000时,111100时,11110时,11110时,11	, 原密钥: 1010000010 ['1010010110', '1011001010', '1011011110'] , 原密钥: 1110001110 ['0100100011', '0100110111', '0101101011', '0101111111', '1111 , 原密钥: 1100110011 ['0001101110', '0001111011', '1101111011'] , 原密钥: 1010101010	1000:	110']	
测试用例 1: 则识:101010100 密文:10001101 替代密钥数量:3 前5个替代密钥: 则试:11001100 密文:11111100 替前5个替代密钥: 则试:1110110011011101111时,111101111时,11110111时,11110000。 密文:11110111时,11110000。 图文:1111001011时,11110000。 图文:111100101时,11110000。 图文:01111001时,11110000。 图文:01111001时,11110000时,11110000时,11110000时,11110000时,11110000时,111100时,11110时,11110时,11	,原密钥: 1010000010 ['1010010110', '1011001010', '1011011110'] ,原密钥: 1110001110 ['0100100011', '0100110111', '0101101011', '0101111111', '111' ,原密钥: 1100110011 ['0001101110', '0001111011', '1101111011'] ,原密钥: 1010101010	10003	110']	

图 4 密钥分析界面

(四) 状态栏

在窗口底部,软件提供状态栏,用于显示当前操作状态(如"加密完成"、 "暴力破解进行中"等),方便用户了解任务执行情况。

密钥冲突分析完成

五、常见问题与错误提示说明

1. 输入长度错误: 必须输入固定长度的二进制字符串(8位或10位)。

- 2. 非法字符:输入中只能包含'0'或'1'。
- 3. 文本加密结果乱码: S-DES 加密输出为二进制字节流,转换为字符时可能显示为不可读符号,可查看十六进制结果。
 - 4. 暴力破解耗时较长: 请耐心等待, 进度条将实时更新。

六、附录: S-DES 算法原理简述

S-DES 是一种教学用途的简化版对称加密算法,通过 10 位主密钥生成两个 8 位子密钥(K1、K2),并对 8 位明文执行两轮 Feistel 结构加密。每轮包括扩展置换、S 盒替换、异或与置换操作。

核心组成包括:

- 密钥生成(P10、P8 置换与循环左移)
- 初始置换(IP)与逆置换(IP⁻¹)
- 轮函数 F(扩展置换 EP、S 盒 SO/S1、P4 置换)
- 轮间交换与异或操作