1 S-DES 工具开发手册

main.py：主要功能函数

1、subkey：密钥生成

功能：根据 10 位密钥生成两个 8 位的子密钥（k1 和 k2）。

参数：origin（list） - 10 位密钥的二进制列表。

返回值：[k1, k2]（list） - 包含两个子密钥的列表。

2、permutation：初始置换函数

功能：对 8 位二进制输入进行初始置换。

参数：origin（list） - 8 位输入的二进制列表。

返回值：p_result（list） - 经过置换后的 8 位二进制列表。

3、permutation_reverse：二次置换函数

功能：对经过加密后数据进行二次置换。

参数：origin（list） - 经过 F 函数处理的二进制列表。

返回值：p_reverse_result（list） - 经过二次置换后的二进制列表。

4、swap：左右互换操作

功能：左右互换操作。

参数：origin（list） - 8 位输入的二进制列表。

返回值：交换后的二进制列表。

5、encryption：加密函数

功能：使用给定的密钥对 8 位明文进行加密。

参数：text（list） - 8 位明文的二进制列表，

key（list） - 10 位密钥的二进制列表。

返回值：ip_str（str） - 加密后的密文字符串。

6、decryption：解密函数

功能：使用给定的密钥对 8 位密文进行解密。

参数：text（list） - 8 位密文的二进制列表，

key（list） - 10 位密钥的二进制列表。

返回值：解密后的 8 位二进制列表。

7、brute_force_decrypt：暴力破解函数

功能：暴力破解函数，用于查找可能的密钥。

参数：cipher_text（list） - 8 位密文的二进制列表。

expected_plain_text（list） - 已知的 8 位明文的二进制列表。

返回值：found_keys（list） - 所有找到的密钥的列表。

8、perform_sdes：执行加密

功能：执行 S-DES 加密过程，处理用户输入并输出密文。

参数：无。

返回值：无（更新界面标签显示密文）。

9、perform_brute_force：执行暴力破解

功能：执行 S-DES 暴力破解过程，处理用户输入并输出找到的密钥。

参数：无。

返回值：无（更新界面标签显示找到的密钥及破解时间）。

10、string_to_binary：将字符串转换为二进制列表

功能：将字符串转换为二进制列表。

参数：input_string（str） - 要转换的字符串。

返回值：binary_list（list） - 由二进制位组成的列表。

11、binary_to_string：将二进制列表转换为字符串

功能：将二进制列表转换为字符串。

参数：binary_list（list） - 由二进制位组成的列表。

返回值：result_string（str） - 还原后的字符串。

12、binary_string_to_list：将 8 位二进制字符串转换为二进制列表

功能：将 8 位二进制字符串转换为二进制列表。

参数：binary_string（str） - 8 位二进制字符串。

返回值：binary_list（list） - 二进制位列表。

13、binary_list_to_string：将二进制列表转换为 8 位二进制字符串

功能：将二进制列表转换为 8 位二进制字符串。

参数：binary_list（list） - 二进制位列表。

返回值：binary_string（str） - 8 位二进制字符串。

14、go_to_encryption：切换到加密界面

功能：切换到 S-DES 加密功能界面。

参数：无。

返回值：无（更新界面显示加密功能相关元素）。

15、go_to_brute_force：切换到暴力破解界面

功能：切换到 S-DES 暴力破解功能界面。

参数：无。

返回值：无（更新界面显示暴力破解相关元素）。

16、clear_frame：清空界面内容

功能：清空当前界面的所有元素。

参数：无。

返回值：无（移除界面上的所有组件）。

17、init_gui：初始化 Tkinter 窗口

功能：初始化 S-DES 工具的 GUI 窗口。

参数：无。

返回值：无（设置窗口标题、尺寸和背景颜色）。

2 用户指南

1. 程序运行

运行 main.py 文件，弹出程序主界面

运行 test.py 文件，实现交叉测试

2. 界面介绍

功能选择：在主界面选择功能，暴力破解或者加密

暴力破解:在暴力破解界面,输入 8 位二进制的密文和已知的 8 位二进制的明文，点击执行按钮，显示破解结果和时间

加密：在加密界面，选择明文输入格式（ASCII 输入或 8 位二进制输入），其次分别输入明文和 10 位二进制密钥。点击执行按钮，显示加密密文和解密结果。