S-DES 加解密系统用户手册

系统简介

S-DES（简化数据加密标准）是一种对称密钥加密算法，用于数据的加密和解密。本系统是一个基于S-DES算法的加解密工具，它提供了一个图形用户界面（GUI），允许用户轻松地加密和解密信息，以及进行暴力破解密钥。

环境配置

操作系统：本系统支持Windows、macOS和Linux操作系统。

Python版本：需要Python 3.x版本。

依赖库：需要安装Tkinter库，用于GUI的构建。

安装步骤

确保Python已安装在您的系统上。

打开终端或命令提示符，安装Tkinter（如果尚未安装）：pip install tk

将tools.py和cipher.py文件保存到您的计算机上。

启动系统

打开终端或命令提示符，导航到包含cipher.py文件的目录。

功能介绍

加密：将明文加密成密文。（包括二进制和ASCII码）

解密：将密文解密回明文。（包括二进制和ASCII码）

暴力破解：通过明密文对来找到全部的加密密钥。

使用说明

加密

点击顶部导航栏的“加密”按钮。

在“请输入明文”输入框中输入您想要加密的文本或二进制字符串。

在“请输入密钥”输入框中输入10位的二进制密钥。

点击“加密”按钮，加密结果将显示在下方的标签中。

解密

点击顶部导航栏的“解密”按钮。

在“请输入密文”输入框中输入您想要解密的文本或二进制字符串。

在“请输入密钥”输入框中输入10位的二进制密钥。

点击“解密”按钮，解密结果将显示在下方的标签中。

暴力破解

点击顶部导航栏的“暴力破解”按钮。

在“请输入明文”输入框中输入原始明文的二进制字符串。

在“请输入密文”输入框中输入对应的密文的二进制字符串。

点击“暴力破解”按钮，系统将尝试找到正确的密钥。破解结果将显示在下方的标签中。

注意事项

确保输入的密钥是10位的二进制字符串。

明文和密文可以是ASCII字符或相应的二进制字符串。

暴力破解功能可能需要一些时间来找到正确的密钥，具体取决于硬件性能。

S-DES 加解密系统开发手册

引言

本开发手册旨在为开发者提供S-DES加解密系统的详细开发指南。本系统使用Python语言开发，提供了一个图形用户界面（GUI），允许用户进行数据的加密、解密以及密钥的暴力破解。

技术栈

编程语言：Python 3.x

图形用户界面库：Tkinter

算法：S-DES 加密算法

主要函数

tools.py

initial\_permutation(Plaintext): 执行初始置换。

inverse\_initial\_permutation(data): 执行最终置换。

key\_Generation(Key): 生成子密钥。

convert\_to\_binary(n): 将数字转换为二进制表示。

f\_function(data, subkey): 执行F函数，包括扩展置换、S盒替换和P4置换。

tow\_round\_encryption(data, subkey1, subkey2): 执行两轮加密。

tow\_round\_decryption(data, subkey1, subkey2): 执行两轮解密。

brute\_force\_cracking(P, C): 执行暴力破解以找到密钥。

cipher.py

is\_valid\_binary\_string(input\_str): 验证输入字符串是否为有效的二进制字符串。

ascii\_str\_to\_binary\_str\_list(ascii\_str): 将ASCII字符串转换为二进制字符串列表。

binary\_str\_list\_to\_ascii\_str(binary\_str\_list): 将二进制字符串列表转换回ASCII字符串。

encrypt(): 加密函数，调用tools.py中的加密相关函数。

decrypt(): 解密函数，调用tools.py中的解密相关函数。

brute(): 暴力破解函数，调用tools.py中的暴力破解相关函数。

功能实现

加密：用户输入明文和密钥，系统通过调用encrypt()函数进行加密。

解密：用户输入密文和密钥，系统通过调用decrypt()函数进行解密。

暴力破解：用户输入明文和密文，系统通过调用brute()函数尝试找到正确的密钥。

性能优化

密钥生成：通过预计算和缓存常用的子密钥，减少重复计算。

并行处理：在暴力破解过程中，可以使用多线程或多进程来加速密钥搜索。

优化S盒：预先计算S盒的结果，以减少运行时的计算量。

算法安全分析

S-DES的密钥长度较短（10位），因此安全性较低，不适合用于高安全需求的场景。

由于S-DES是DES的简化版，它继承了DES的一些已知弱点，如差分密码分析和线性密码分析。