用户指南

#### [1.概述](https://github.com/guangying666/S-DES#1%E6%A6%82%E8%BF%B0)

1.1 项目介绍

本项目名为S-DES加密解密系统。采用轻量级的对称加密算法 S-DES（Simplified Data Encryption Standard），能够对数据的安全进行一定的保护。该算法由美国圣克拉拉大学的Edward Schaefer教授于1996年提出，适用于教育用途。

1.2 用户指南概览

本用户指南将帮助您了解如何本项目的数学原理和使用流程。

#### [2.数学基础](https://github.com/guangying666/S-DES#2%E6%95%B0%E5%AD%A6%E5%9F%BA%E7%A1%80)

2.1 本项目的运行原理

本项目采用S-DES算法，明文分组为8位，主密钥分组为10位，采用两轮选代。

2.3 密钥生成

利用随机种子随机生成一个10bit密钥

#### 2.2 加密和解密[2.数学基础](https://github.com/guangying666/S-DES#2%E6%95%B0%E5%AD%A6%E5%9F%BA%E7%A1%80)

2.1 本项目的运行原理

本项目采用S-DES算法，明文分组为8位，主密钥分组为10位，采用两轮选代。

2.3 密钥生成

利用随机种子随机生成一个10bit密钥

2.2 加密和解密

#### [2.数学基础](https://github.com/guangying666/S-DES#2%E6%95%B0%E5%AD%A6%E5%9F%BA%E7%A1%80)

2.1 本项目的运行原理

本项目采用S-DES算法，明文分组为8位，主密钥分组为10位，采用两轮选代。

2.3 密钥生成

利用随机种子随机生成一个10bit密钥

2.2 加密和解密

加密算法：输入铭文和密钥，执行加密操作得到密文

解密算法：输入密文和正确的密钥，执行解密操作得到铭文

2.4 暴力破解

遍历所有密钥，直到找到符合要求的密钥

2.5gui界面



1. 使用S-DES加密数据

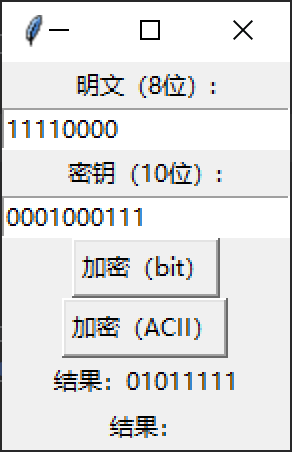
3.1准备工作

首先，您需要一个密钥，可通过以下方式获取：

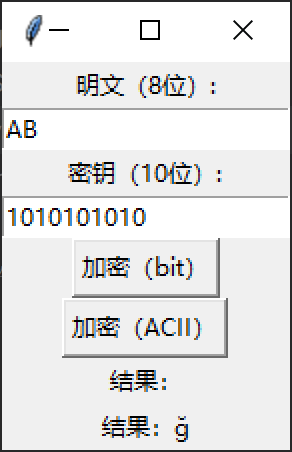
自行准备一个有效的S-DES密钥（10bit）。

通过获取密钥功能获取一个随机密钥

3.2示例：如何使用S-DES加密二进制数据



3.2示例：如何使用S-DES加密ASCLL字符串

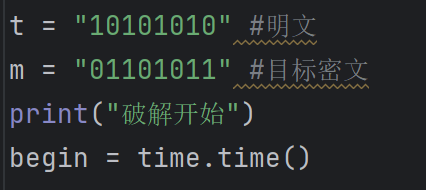


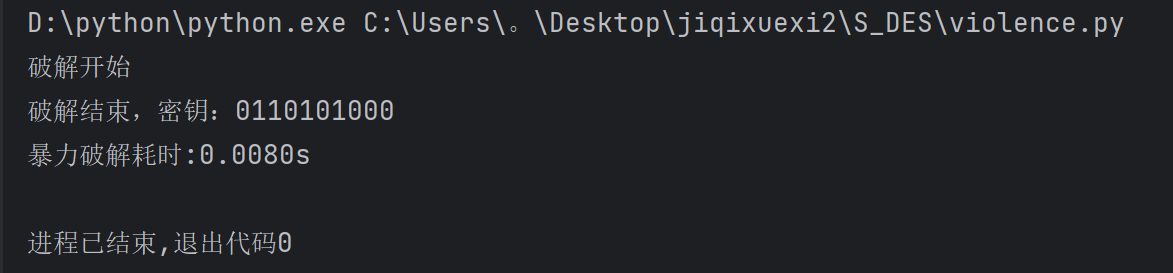
1. 解密数据

首先，您需要一个密钥，可通过以下方式获取：

获取一个个有效的S-DES密钥（10bit）。

准备要解密的密文数据



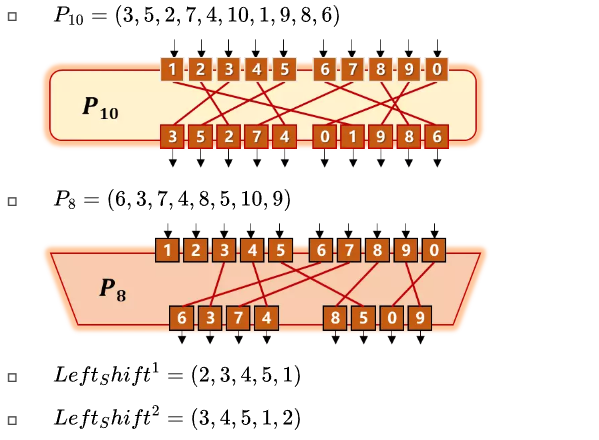


1. S-DES的参数设置

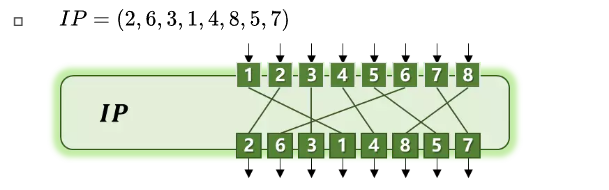
5.1密钥长度

1. DES使用二进制10bit密钥

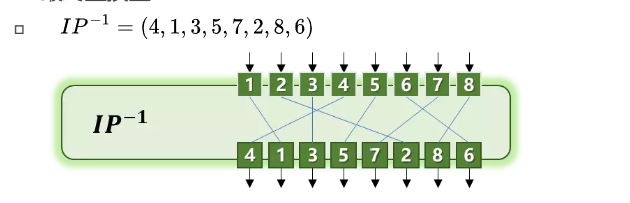
5.2密钥扩展置换



5.2初始置换盒



5.3最终置换盒



5.4轮函数

