

**DES加密解密程序用户指南**

**目录**

**1引言**

**2软件概述**

**2.1功能介绍**

**2.2系统架构**

**2.2.1程序**

**2.2.2界面和使用说明**

**3运行环境**

**1引言：**

S-AES（Simplified Advanced Encryption Standard）是一种轻量级对称密钥加密算法，旨在提供基本数据保护功能。它采用固定大小的数据块，执行基本的替代和置换步骤，支持不同的运算模式，但由于其轻量级性质，不适合处理高度敏感的机密数据。通常用于教育和研究，以帮助理解对称密钥加密的基本概念和算法。如果需要更高级的数据安全性，通常会选择更复杂的加密标准，如 AES。

**2软件概述：**

**2.1功能介绍**

本程序可以实现S-AES加密解密算法，使用者可以通过16位的密钥对16位的明文或密文进行加密和解密操作

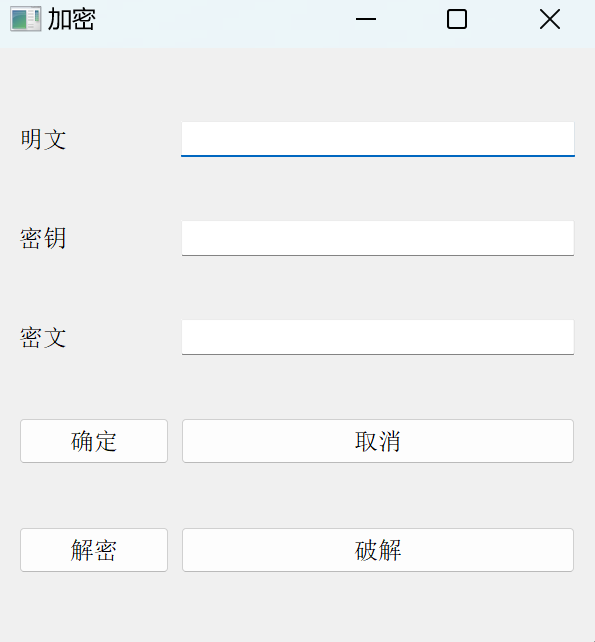
**2.2系统架构：**

**2.2.1程序：**

分组长度16，密钥长度16。代码有相应注释。逐步实现了S-AES加密解密算法。

**2.2.2界面：**

菜单栏可以放缩程序和直接缩小关闭程序。如图1、2：使用者可以在明文栏输入想加密的明文，在密钥行输入密钥，在加密状态下可以得到相关密文。可以点击解密/加密按钮切换加密解密模式。点击破解可以通过一组明密文对得到对应的密钥，切换到破解界面如图3所示。

** **

**图1 图2**



**图3**

**3.运行环境：**

Pycharm

Windows10,11

库：python3.11.4， pyqt5， sys， math