

**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：**

数据加密标准（Data Encryption Standard，DES） 是一种对称密钥加密算法，最早由IBM于上世纪70年代开发。虽然在现代密码学中已经被更强大和安全的算法所取代，但DES仍然具有历史意义和重要性，它在教育和研究，帮助对称密钥密码学的理解，设计安全性评估仍然发挥其作用

**2软件概述：**

**2.1功能介绍**

本程序可以实现DES加密解密算法，使用者可以自行设计10位的密钥对8位的密码进行加密和解密操作

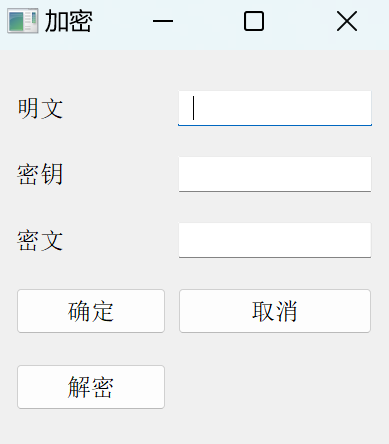
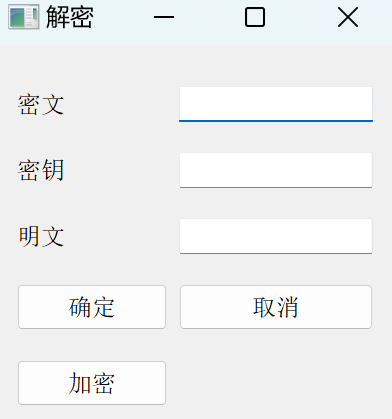
**2.2系统架构：**

**2.2.1程序：**

分组程度8bit，密钥长度10bit。代码有相应注释。逐步实现了完备的DES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。

** **

**图1 图2**

**3.运行环境：**

Pycharm

Windows10,11

库：python3.11.4， pyqt5， sys， math