**项目名称**

**介绍：**

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

**项目的目的和范围**

本项目旨在通过des算法学术学习和理解密码，学加强编程技能，增加对加密算法的安全性理解和理解加密标准。

**环境配置**

提供开发和部署所需的环境配置说明，包括操作系统、软件、库等。

系统：Windows

环境：pycharm

库：sys， math， pyqt5

**开发规范**

**1** 变量命名规范使用有意义的名字来为变量、函数和类命名，描述其用途。使用驼峰命名法（CamelCase）或下划线分隔命名法（snake\_case）。使用描述性的名字，避免使用单个字符的变量名，除非是临时变量。

**2** 代码注释使用各编程语言对应的符号进行单行或多行注释，在注释中需使用清晰、有意义的语言，用于解释单行代码或代码块的功能、算法或特定说明（如代码的创新）。同时避免过多的注释，只需复制相对复杂或不明显的部分。

**3** 函数式编程使用函数式编程，将代码模块化，每个小模块负责特定的功能实现。对于重复的代码，可以使用函数或类来实现代码的复用，推荐使用标准库和第三方库辅助算法的实现。

**架构设计**

系统分为程序和界面两部分。

**程序主体实现了des的细节**

输入（Plaintext）： 这是要加密的原始数据，也就是需要保密的信息。在DES中，明文通常以64位二进制形式表示。

密钥（Key）： 密钥是一个关键的组成部分，用于加密和解密数据。在DES中，密钥的长度为56位，但实际上是64位中的8位用于奇偶校验，因此只有56位是用于实际加密的关键部分。

初始置换（Initial Permutation，IP）： 明文输入首先通过初始置换，将输入的64位数据重新排列，以作为加密的初始数据。

轮函数（Round Function）： DES使用轮函数来进行数据混淆和替代操作。轮函数接收一组数据和一个轮密钥，对数据进行变换，然后输出数据。DES共有16轮加密过程，每一轮使用不同的轮密钥。

轮密钥（Round Keys）： 在DES中，根据主密钥生成16个轮密钥。每个轮密钥都是从主密钥派生出来的，用于每轮的加密和解密操作。

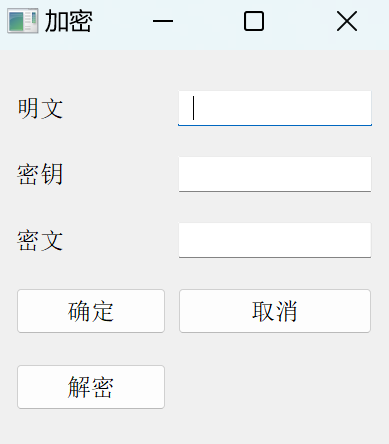
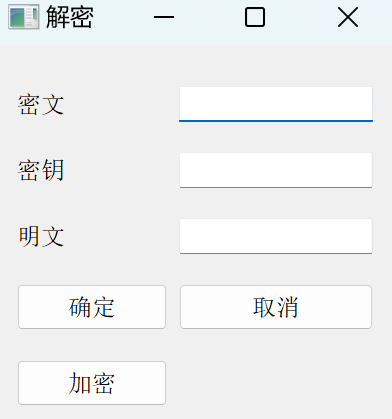
S-盒（S-Boxes）： S-盒是DES中的核心元素，用于替代和混淆数据。DES有8个不同的S-盒，每个S-盒都将输入的6位数据映射为4位输出数据，以便进一步的混淆。

P-盒（P-Box）： P-盒用于混淆数据，将轮函数的输出重新排列以作为下一轮的输入。

交替结构： DES使用了交替结构，即轮函数的输出与前一轮的数据交替进行XOR运算。这种交替结构增加了加密的复杂性和安全性。

最终置换（Final Permutation，FP）： 在DES加密结束后，密文通过最终置换进行重新排列，以生成最终的加密结果。

在**应用界面**部分实现了给程序使用者进行交互的界面如图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**