

# 开发手册

## 1. 简介

本次开发是基于 S-DES 算法和 Python+QT 语言编程实现加密，解密算法，以及暴力破解等内容。

开发人员为：于大泉，胡雨丹，主要职责为算法编写，界面设计以及文档书写。

使用的开发环境为 Windows 系统以及 pycharm、Visual Studio Code 开发工具，用以编程实现算法和界面设计。

## 2. 总体设计以及界面介绍

本次主要设计实现加密，解密以及暴力破解三个功能，通过输入明文，密钥和密文等内容，能够实现以上三个内容。同时为了实用性扩展符文加密功能。本次的界面设计如下，功能按键如图所示：



## 3. 文件结构和接口设计

(1) encrypt.py：实现加密解密算法，同时实现了 ASCII 码扩展部分加解密

permute：置换函数

`binary_to_decimal`：二进制转化为十进制

`decimal_to_binary`：十进制转化为二进制

`replace`：替换操作

`class Encryptor`：封装了加密解密的内容的 `class` 类，其中的函数包含以下部分：

`generate_key`：随机生成 10bit 密钥的函数

`set_key`：保存输入的密钥

`generate_subkey`：生成子密钥

`single_group_encrypt`：明文加密函数

`F_function`：轮函数

`encrypt_string`：加密（解密）函数，支持字符串输入，生成 ASCII 密文

`encrypt_binary`：二进制列表输入的加密解密函数

## (2) `decrypt.py`：实现暴力破解

`class Decryptor`：解密算法类，函数包含与加密一致

`class CrackThread`：使用线程暴力破解密钥的 `class` 类，包含以下函数：

`find_key`：通过穷举法暴力破解得到可能密钥的函数

`progress_bar`：建立进度条查看解密进度

`sift`：多个明密文对的密钥筛选得到共同密钥的函数

`onethread`：寻找一对密钥的函数

`Multithreading`：创建多个线程，寻找明密文对密钥的函数

`solve`：启动线程寻找明密文对

(3) `ui`：实现界面设计，包括三个主要功能的页面图形等

(4) `main.py`：主函数，直接实现界面交互功能

#### 4. 第三方组件

引用的插件

```
import sys
```

```
from PyQt5.QtWidgets import QApplication
```

```
from PyQt5.QtCore import pyqtSignal
```

```
import random
```

```
import threading
```

```
import time
```