开发手册

1. 简介

本次开发是基于 S-AES 算法和 Python+QT 语言编程实现加密，解密算法，其中 S-AES 算法基于于密码编码学与网络安全--原理与实践第八版的附录五，本次同时实现多重加密中间相遇攻击和 CBC 分组加密等内容。

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。本次的界面设计使用有效，展示如下，功能按键如图所示：

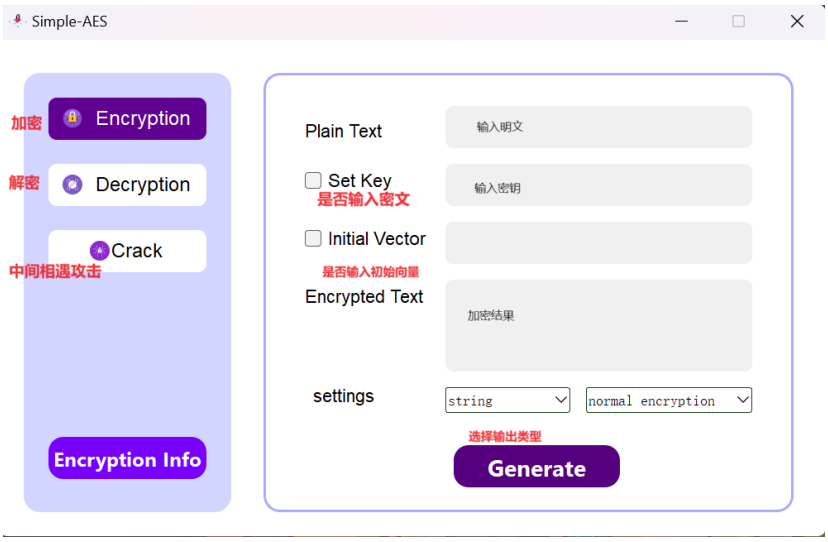

图 1 交互界面

3. 文件结构和接口设计

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

text16bit_to_nibble_matrix: 将 16 位数据划分为半字节矩阵

nibble_matrix_to_text16bit: 将半字节化为 16 位矩阵

get_bit_vector: 获取位向量

vector_to_num：矢量化为整数

class AES：封装了加密解密及 CBC 分组加密的内容的 class 类，其中的函数包含以下部分：

generate_key：生成密钥的函数

set_key：保存输入的密钥

encrypt: 加密程序

set_initial_vector: 初始化密钥

set_key：设置初始密钥

decrypt：解密函数

string_encrypt：加密函数，支持字符串输入，生成 ASCII 密文

string_decrypt：解密 ASCII 的输入函数

group_encrypt：明文组加密

group_decrypt：密文组解密

__add_key：密钥加函数

__nibble_replace：半字节替换

_shift_row：行位移

__mix_col：列混淆

__extend_keys：密钥扩展

generate_vector：向量生成

__generate_sbox：生成 sbox

(2) multiple.py：实现多重加解密和中间相遇攻击

class multiple：实现二重加密和和三重解密的 class 类，包含以下函数：

two_encrypt：二重加密函数

two_decrypt：二重解密函数

try_ck：中间相遇攻击中对密文破解函数

try_pk：中间相遇攻击对明文破解函数

find_onegroup：对一对明密文对进行中间相遇攻击

find_mid：中间相遇攻击函数

three_two_encrypt：三重加密函数

three_two_decrypt：三重解密函数

（3）ui：实现界面设计，包括几个主要功能的页面等

（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 ui.src.window_controller import WindowController

from PyQt5.QtCore import pyqtSignal

import random
```