介绍：

S-AES是信息安全导论作业小组（成员：蒋铭皓，郭景逸）制作的基于S-AES规则的加解密程序，旨在提供安全可靠的数据加解密服务。

软件架构：

本项目的软件架构采用模块化设计，每个模块之间通过接口进行交互。

本项目的模块：

界面模块：提供用户界面，实现用户与程序的交互。界面模块采用图形界面等方式实现，包括输入密钥、选择加解密模式、显示明文/密文等操作，在jiemian.py中实现，jiemian.ui是原始的ui文件；

单重加解密模块：实现S-AES加解密算法的核心部分，算法在S\_AES.py中实现；

单重加解密字符输入输出模块：向实用性扩展，加密算法的数据输入可以是ASII编码字符串(分组为2 Bytes)，对应地输出也可以是ACII字符串，算法在S\_AES\_string.py中实现

双重加解密模块：基于S-AES加解密算法实现双重加解密并返回明文/密文，算法在S\_AES.py中实现；

三重加解密模块：基于S-AES加解密算法实现三重加解密并返回明文/密文，算法在S\_AES.py中实现；

CBC模式模块：实现在S-AES算法下的CBC模式加解密，算法在S\_AES.py中实现；

中间相遇攻击模块：实现了对S-AES加解密下的多个明密文对的中间相遇攻击，此模块未加入ui界面。

single\_meet\_middle\_attack.py是单对明密文中间相遇攻击，multiple\_meet\_middle\_attack.py是多对明密文中间相遇攻击

安装教程：

本项目暂未提供exe安装包。下载项目文件后运行文件main.py即可打开程序。

运行环境:

python3.10.12

pyside6 6.6.0

使用说明

ui界面使用说明：

主界面：按照界面上的文本标识，在对应的文本框中输入明文\密文与密钥，点击加密/解密按钮进行操作，在输出文本框获取加密/解密的结果；

各个加解密模式使用说明：

单重加密：此模式实现基础的S-AES加解密。要求输入的明/密文与密钥均为16位的二进制数。

字符串加密：此模式实现基础的S-AES加解密，并将加解密后的的密/明文转换的ASCII字符串。要求输入的明密文与密钥均为16位的二进制数。

=双重加密：此模式实现基于S-AES的双重加解密。要求输入的明/密文为16位的二进制数，输入的密钥为32位的二进制数。

三重加密：此模式实现基于S-AES的三重加解密。要求输入的明/密文为16位的二进制数，输入的密钥为48位的二进制数。

CBC加密：此模式实现在S-AES算法下的CBC模式加解密。要求输入的明/密文与密钥均为16\*k位的二进制数（k为正整数），且明/密文与密钥的位数一致。

参与贡献

郭景逸：ui界面设计与制作、S-AES基础算法代码实现、中间相遇攻击代码实现、实验报告撰写

蒋铭皓：双重加解密代码实现、三重加解密代码实现、中间相遇攻击代码实现、CBC模式代码实现、项目文档撰写