**S-AES 加密解密系统 - 用户指南**

# 项目介绍

基于S\_AES加密解密算法，实现其基本功能，并拓展实现了支持ASCII码的加密解密功能，支持双重三重加密解密，利用相遇攻击破解双重加密密钥的功能，最后还完成了CBC工作模式并探索其性质。

# 技术栈：

python+qt

# 使用方式：

## 环境要求：

- python 3.9

- pyqt5 5.15.11

## 安装依赖

- pip install -r requirements.txt

## 运行程序

- python main.py

# 界面介绍

## 基础加密解密界面

- 输入16bit二级制明文与密钥，或者4位十六进制明文与密钥

- 输出16bit二级制密文与4位十六进制密文

- 输出解密后的明文

## ASCII加密解密界面

- 输入ascii码文本

- 输出密文

- 输出解密后的明文

## 双重加密解密界面

- 输入明文与两个密钥k1,k2

- 输出双重加密（\*\*C=(E(k2,E(k1,P)))\*\*）后的密文

- 输出双重解密（\*\*P=(D(k1,D(k2,C)))\*\*）后的明文

## 中间相遇攻击界面

输入明文密文

输出找到相同mid\_text的可能密钥对k1,k2

## 三重加密解密界面

- 输入明文与三个不同的密钥k1,k2,k3

- 输出三重加密（\*\*C=(E(k3,E(k2,E(k1,P))))\*\*）后的密文

- 输出三重解密（\*\*P=(D(k1,D(k2,D(k3,C)）))\*\*）后的明文

## CBC工作模式界面

- 输入明文，密钥，初始向量

- 输出密文块

- 输出修改第一个密文块后再解密的明文

# 目录结构

```

s\_aes/

├── main.py # 程序主入口

├──s\_aes\_corepy # 基础加密逻辑

├── s\_aes\_mode.py # 双重，三重，CBC模式功能的逻辑

├── gui.py # 交互界面

├── s\_aes.docx # 帮助文档

└── requirements.txt # 依赖项

```

# 帮助文档：

- s\_aes.docx