用户指南

1. 运行程序

(1) 克隆仓库代码

```
git clone https://github.com/HJingCheng/S-AES.git
```

(2) 安装依赖

```
pip install -r requirements.txt
```

(3) 启动程序

```
python app.py
```

(4) 在浏览器打开http://localhost:5000 访问Web界面

2. 基本加解密

在"加解密"标签页中,可以进行以下操作:

- 输入16进制的明文和密钥,点击"加密"按钮进行加密,点击"解密"按钮进行解

加密	解密
	

- 选择"ASCII"选项,可以输入任意长度的ASCII字符串进行加密和解密

ASCII加密	解密
	

- 选择"双重加密",可以输入16进制明文和32位十六进制密钥,进行双重加密和解密

双重加密

解密

- 选择“三重加密”,可以输入16进制明文和48位十六进制密钥,进行三重加密和解密

三重加密

解密

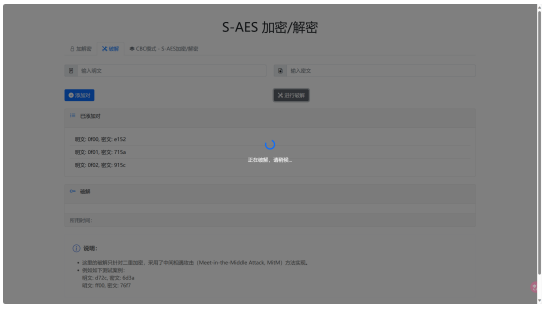
3. 破解

在“破解”标签页中,可以进行中间相遇攻击,步骤如下:

- 输入明文和密文组成一对,点击"添加对"按钮
- 重复上述步骤,添加多个明密文对

- 点击“进行破解”按钮,会显示破解得到的密钥`K1`和`K2`,以及破解耗时

等待破解



成功破解

4. CBC模式加解密

在“CBC模式”标签页中,可以进行CBC模式的加解密:

- 输入16进制密钥和初始向量`IV`
- 在长明文输入框中输入要加密的明文
- 点击“CBC加密”按钮进行加密,结果会显示在结果区域

- 可以点击展开按钮,添加或者修改密文
- 点击“CBC解密”按钮进行解密,查看修改前后解密结果的比较

篡改前	进行篡改测试