一、用户指南

1. 系统概述

S-AES 加密系统是基于简化版 AES（S-AES）算法实现的加密工具，支持基础加密、ASCII 文本加密、双重加密、三重加密、中间相遇攻击模拟及 CBC 工作模式，提供可视化操作界面和调试功能，适用于密码学教学与算法验证。

2. 安装与运行

环境要求：Python 3.6+，需安装numpy库（可通过pip install numpy安装）

运行方式：直接执行脚本文件，系统将自动启动图形界面

3. 功能模块使用说明

3.1 基础加密

功能：实现 16 位二进制明文的加密与解密

操作步骤：

在 “明文” 框输入 16 位二进制字符串（如0110111101101011）

在 “密钥” 框输入 16 位二进制密钥（如1010011100111011）

点击 “加密” 生成密文，点击 “解密” 验证还原结果

点击 “填充示例” 可加载预设测试数据

3.2 ASCII 加密

功能：对 ASCII 字符串（如英文、数字、符号）进行加密解密

操作步骤：

在 “ASCII 文本” 框输入字符串（如Hello AES!）

输入 16 位二进制密钥

点击 “加密” 生成乱码形式的密文，点击 “解密” 还原原始文本

3.3 双重加密

功能：使用 32 位密钥（分两个 16 位子密钥）进行两次加密

操作步骤：

输入 16 位二进制明文和 32 位二进制密钥（如10100111001110111010011100111011）

点击 “加密” 生成密文，点击 “解密” 验证

3.4 三重加密

功能：支持 32 位密钥（K1-K2-K1 模式）和 48 位密钥（K1-K2-K3 模式）的三重加密

操作步骤：

选择密钥模式（32 位 / 48 位）

输入 16 位明文和对应长度的密钥

点击 “加密”“解密” 完成操作

3.5 中间攻击

功能：模拟对双重加密的中间相遇攻击，通过已知明文和密文破解密钥

操作步骤：

输入已知 16 位明文和对应密文

设置 “最大测试密钥数”（默认 1000，最大 65536）

点击 “执行攻击”，结果将显示可能的密钥对

3.6 CBC 模式

功能：实现密码分组链接（CBC）模式的加密，验证分组依赖特性

操作步骤：

输入多个 16 位明文分组（空格分隔）、16 位密钥和 16 位初始向量 IV

点击 “加密” 生成密文分组，点击 “解密” 还原

点击 “篡改测试” 可验证篡改一个密文分组对后续结果的影响

3.7 正确性测试

功能：验证算法实现的正确性，包括标准测试、S 盒验证、列混淆验证和交叉测试

操作步骤：点击对应按钮，结果将显示在下方文本框中

4. 调试功能

点击 “开启调试” 可在底部输出框显示算法执行过程（如轮密钥生成、状态矩阵变换）

点击 “关闭调试” 停止输出，“清空输出” 可清除调试信息