# 用户手册

### 1. S-AES加密程序(GUI版本)

程序概述

该程序实现了基于S-AES算法的加密过程，并提供了图形用户界面以便用户进行交互。用户可以输入16位的数据和16位的密钥，程序将输出对应的16位密文。此外，程序支持ASCII编码字符串的输入，程序会将字符串分组为2字节进行加密，并输出可能呈现为乱码的ASCII字符串作为密文。

使用指南

打开程序后，您会看到两个输入框：一个用于数据输入，一个用于密钥输入。

输入您的16位数据和16位密钥。如果您输入的是ASCII字符串，确保它可以被分为2字节的块。

点击“加密”按钮，程序将显示16位密文。

如果需要解密，将密文输入数据框，保持密钥不变，点击“解密”按钮。

注意事项

确保输入的数据和密钥格式正确。

对于ASCII字符串，程序会自动处理分组。

### 2. 双重S-AES加密程序

程序概述

此程序通过对S-AES算法进行双重加密来增强安全性。分组长度为16位，密钥长度为32位。

使用指南

在数据输入框中输入16位分组数据。

在密钥输入框中输入32位密钥（将被内部分为两个16位密钥）。

点击“双重加密”按钮，程序将输出密文。

若要解密，请输入密文并点击“双重解密”按钮。

注意事项

确保密钥长度正确，为32位。

### 3. 中间相遇攻击程序

程序概述

该程序尝试通过中间相遇攻击来找到使用S-AES加密的正确的32位密钥（K1+K2）。

使用指南

输入已知的明文和对应的密文对。

点击“攻击”按钮。

程序将尝试找出正确的密钥，并将结果展示出来。

注意事项

此方法可能需要较长时间，并且成功率取决于已知明密文对的数量和质量。

### 4. 三重S-AES加密程序

程序概述

该程序将S-AES算法通过三重加密进行扩展，使用48位的密钥（K1+K2+K3）。

使用指南

输入16位分组的数据。

输入48位的密钥。

点击“三重加密”按钮，程序将输出密文。

若要解密，请输入密文并点击“三重解密”按钮。

注意事项

密钥必须精确地为48位。

### 5. S-AES的CBC模式加密程序

程序概述

该程序使用密码分组链(CBC)模式对长明文消息进行加密。需要用户注意初始向量(IV)的生成和共享。

使用指南

输入要加密的长明文消息。

输入16位的密钥以及16位的初始向量(IV)。

点击“CBC模式加密”按钮，程序将输出密文。

若要解密，输入密文、相同的密钥及IV，并点击“CBC模式解密”按钮。

如需测试篡改，对密文进行替换或修改后，尝试解密，并对比结果。

注意事项

IV必须是随机生成的，且加密解密双方都要知晓。

篡改密文可能会导致解密失败或结果错误。

以上是对五个程序的基础操作指南。用户在使用过程中应确保输入的数据格式符合