**用户指南：S-AES 解密/加密工具**

**概述**

本工具是一个基于简化版的数据加密标准（S-AES）的加密/解密程序，它与AES的性质和结构类似，但使用的参数更少。AES算法是一种对称加密算法，它在加密和解密时使用相同的密钥或可以简单相互推算的密钥对。AES算法以其128位、192位和256位的密钥长度提供了强大的加密强度，能够有效抵御各种攻击手段，被认为是目前最安全和最常用的加密算法之一。

**S-AES解密/加密工具特点**

1. **高效性**：AES算法本身具有高效性，S-AES解密/加密工具进一步优化了加密和解密过程，使得处理速度更快，满足大数据量加密的需求。
2. **安全性**：工具严格遵循AES算法标准，采用高强度的密钥管理和加密模式，确保数据在加密和解密过程中的安全性。同时，支持多种工作模式（如ECB、CBC等）和填充模式（如PKCS7、NONE等），以适应不同场景下的加密需求。
3. **易用性**：S-AES解密/加密工具通常提供图形用户界面（GUI），用户无需编写复杂的代码，只需通过简单的操作即可完成加密和解密任务。此外，还支持多种操作系统和平台，方便用户在不同环境下使用。
4. **兼容性**：工具支持多种密钥长度和加密模式，可以与其他AES加密工具或库进行兼容，方便用户在不同系统之间进行数据交换和共享。

本程序允许用户输入一个 16 位的明文（或ASII编码字符串）和一个 16 位的密钥，然后输出加密或解密后的 对应结果。

**使用步骤**

**1. 准备输入**

密文/明文：输入一个 16 位的二进制字符串（只包含 0 和 1）或ASII编码字符串。例如，1010101010101010、hello,world。

密钥：输入一个 16 位的二进制字符串（只包含 0 和 1）。例如，0101010101010101。

**2. 输入数据**

按照所需要求输入密文/明文。

紧接着输入 16 位的密钥。

**3. 运行程序**

在UI界面中点击对应功能按钮运行程序。

**4. 查看结果**

程序将输出加密/解密后的对应结果。

**注意事项**

确保输入的密文/明文和密钥都是有效的 16 位二进制字符串或ASII编码字符串。

如果输入格式不正确（例如，包含非二进制字符或长度不正确），程序将显示错误消息并退出。

本程序仅适用于 S-AES 加密/解密过程，不适用于标准的 AES 或其他加密算法。

**示例**

**输入示例**

明文：0110111101101011；

密钥：1010011100111011；

得到密文：0000011100111000。

**输出示例**



**解密：**

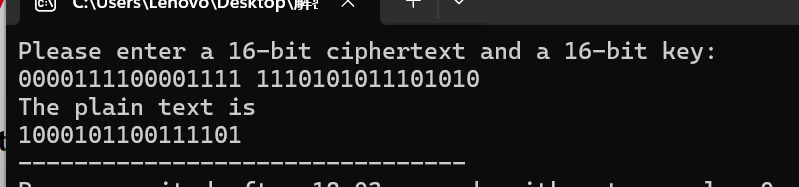
**输入示例**

密文：0000111100001111;

密钥：1110101011101010；

得到明文：1000101100111101

**输出示例**



请注意，输出取决于输入的密文/明文和密钥，以及 S-DES 加密/解密算法的具体实现。

**代码功能简述**

* encrypt(): 主加密函数，调用其他函数执行加密过程，并在页面上显示结果。
* encrypt2(mw, key): 加密函数，接受明文和密钥作为参数，返回密文。
* generateIv(): 生成一个随机的16位初始向量（IV）。
* cbcEncrypt(): CBC模式加密函数，使用初始向量和密钥对明文进行加密。
* cbcDecrypt(ciphertext, key, iv): CBC模式解密函数，使用密文、密钥和初始向量进行解密。
* tamperCiphertext(ciphertext, index, newBlock): 篡改密文分组的函数。
* get(): 获取前端输入的密钥和明文。
* expansion(): 扩展密钥的函数。
* key\_expansion(key): 密钥扩展函数，根据输入的密钥生成扩展密钥。
* hexToBin(hexStr): 将十六进制字符串转换为二进制字符串的函数。
* MC(str): 列混淆函数，对输入的字符串进行矩阵乘法操作。
* NS(str): 半字节替代函数，使用S盒对输入的字符串进行替换。
* SR(str): 行移位函数，对输入的字符串进行循环移位操作。
* hexXOR(str1, str2): 异或操作函数，对两个十六进制字符串进行异或操作。
* binaryToHex(binaryStr): 将二进制字符串转换为十六进制字符串的函数。

本用户手册提供了使用 S-AES 加密/解密工具的基本指南，包括输入要求、运行步骤和注意事项。通过遵循这些指南，用户可以轻松地对数据进行S-AES加密或解密。