第 1 关 基本测试

根据 S-AES 算法编写和调试程序，提供 GUI 解密支持用户交互。输入可以是 16bit 的数据和 16bit 的密钥，输出是 16bit 的密文。

1.加密操作验证

输入一个明文 P：1100100101000111
密钥 K：0010110101010101
得到密文 C：1010011001111101

2.解密操作验证

输入第一步中加密得到的密文 P:1010011001111101
密钥 K:0010110101010101
得到与第一步相同的明文 P:1100100101000111

第 2 关：交叉测试

考虑到是"算法标准"，所有人在编写程序的时候需要使用相同算法流程和转换单元(替换盒、列混淆矩阵等)，以保证算法和程序在异构的系统或平台上都可以正常运行。
设有 A 和 B 两组位同学(选择相同的密钥 K)；则 A、B 组同学编写的程序对明文 P 进行加密得到相同的密文 C；或者 B 组同学接收到 A 组程序加密的密文 C，使用 B 组程序进行解密可得到与 A 相同的 P。

1.我方加密结果

明文 P：1100100101000111
密钥 K：0010110101010101
得到密文 C：1010011001111101

2. 对方加密结果

明文 P：1100100101000111
密钥 K：0010110101010101
得到同样密文 C：1010011001111101

3. 我方解密结果

密文 C：1010011001111101
密钥 K：0010110101010101

得到明文 P：1100100101000111

4. 对方解密结果

密文 C：1010011001111101
密钥 K：0010110101010101
得到同样明文 P：1100100101000111

第 3 关：扩展功能

考虑到向实用性扩展，加密算法的数据输入可以是 ASII 编码字符串(分组为 2 Bytes)，对应地输出也可以是 ACII 字符串(很可能是乱码)。

1.加密验证

输入字符串 P：HelloWorld
密钥 K：0010110101010101
得到密文 C:é VÍÇoíL¶È

2.解密验证

输入字符串 C：HelloWorld
密钥 K：0010110101010101
得到明文 P:éVÍÇoíL¶È

第 4 关：多重加密

4.1 双重加密

将 S-AES 算法通过双重加密进行扩展，分组长度仍然是 16 bits，但密钥长度为 32 bits。

1.

输入明文 1010011100111011

分密钥 1 和密钥 2，输入 32bits 密钥 0011100111001010　　0100111001011010

执行双重加密结果为 1000101111110000

4.2 中间相遇攻击

假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用中间相遇攻击的方法找到正确的密钥 Key(K1+K2)。
因为攻击算法太复杂，所以只生成一种可能存在的密钥 Key
当输入一个明、密文对时：
已知明文：0110111101101001
已知密文：1101111011010110
攻击结果： '0000000000000000', '0001111110010111'

当输入两个明、密文对时：
已知明文：0110111101101001，1101111011010011

已知密文：1101101001010000，1101111011010110
攻击结果：'0000000000000000','0000010101101100'

4.3 三重加密

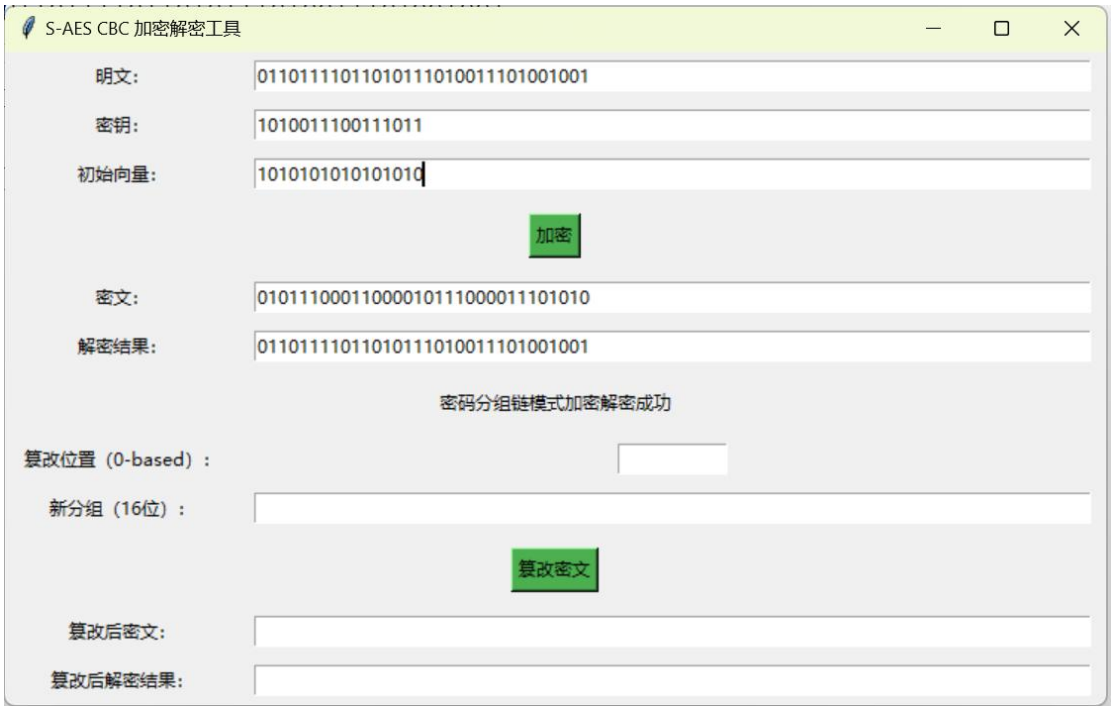
将 S-AES 算法通过三重加密进行扩展，按照 32 bits 密钥 Key(K1+K2)的模式进行三重加密解密
明文：0110111101101001
密钥：1101101001010000 0000010101101100
三重加密结果：1101011111001000

第 5 关：工作模式

基于 S-AES 算法，使用密码分组链(CBC)模式对较长的明文消息进行加密。注意初始向量(16 bits) 的生成，并需要加解密双方共享。
在 CBC 模式下进行加密，并尝试对密文分组进行替换或修改，然后进行解密，请对比篡改密文前后的解密结果。

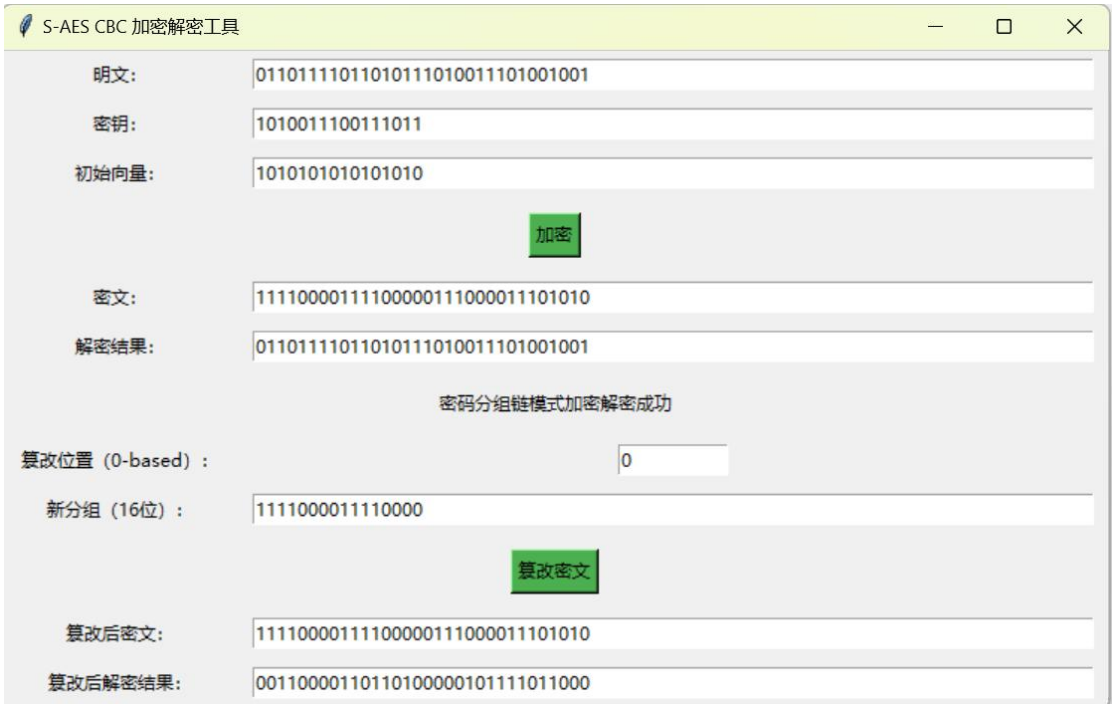
1、CBC 加密

输入明文：01101111011010111010011101001001
　　密钥：1010011100111011
　　初始向量 (IV)：1010101010101010
点击“加密”按钮
加密后的密文为：01011100011000010111000011101010



2、篡改密文

在“篡改位置”输入框中输入要篡改的密文分组的位置（从 0 开始）。例如，输入 0 表示篡改第一个分组。
在“新分组”输入框中输入新的 16 位二进制分组。例如，输入 1111000011110000。
点击“篡改密文”按钮
篡改后的密文：11110000111100000111000011101010



对比篡改密文前后的解密结果

篡改前解密结果：01101111011010111010011101001001
篡改后解密结果：00110000110110100000101111011000