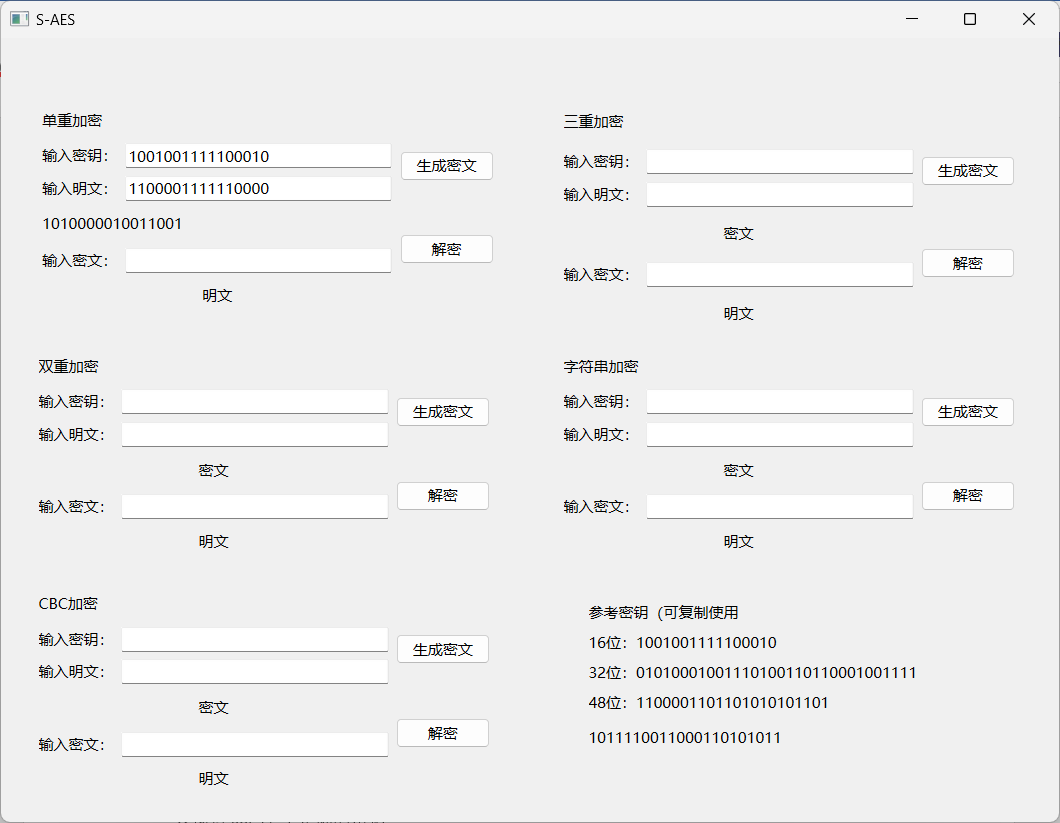
**编程和测试要求**

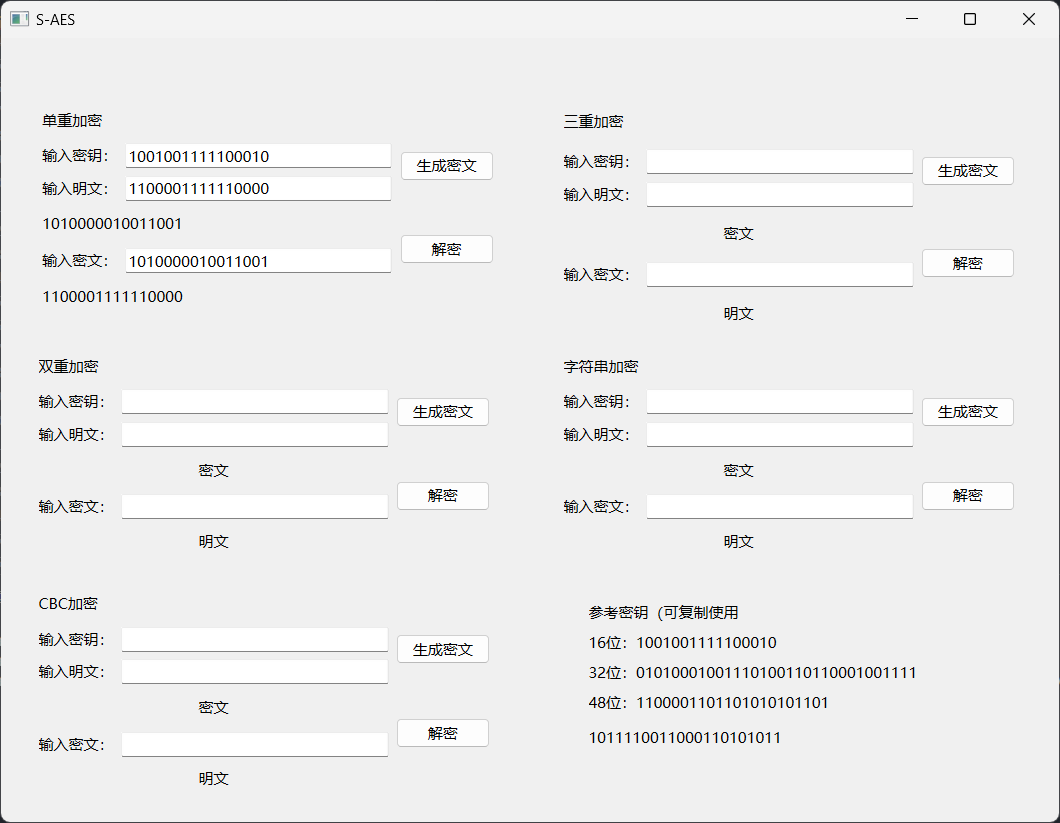
第一关 基本测试

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。

输入16bit明文，16bit密钥加密



输入16bit密文，16bit密钥解密

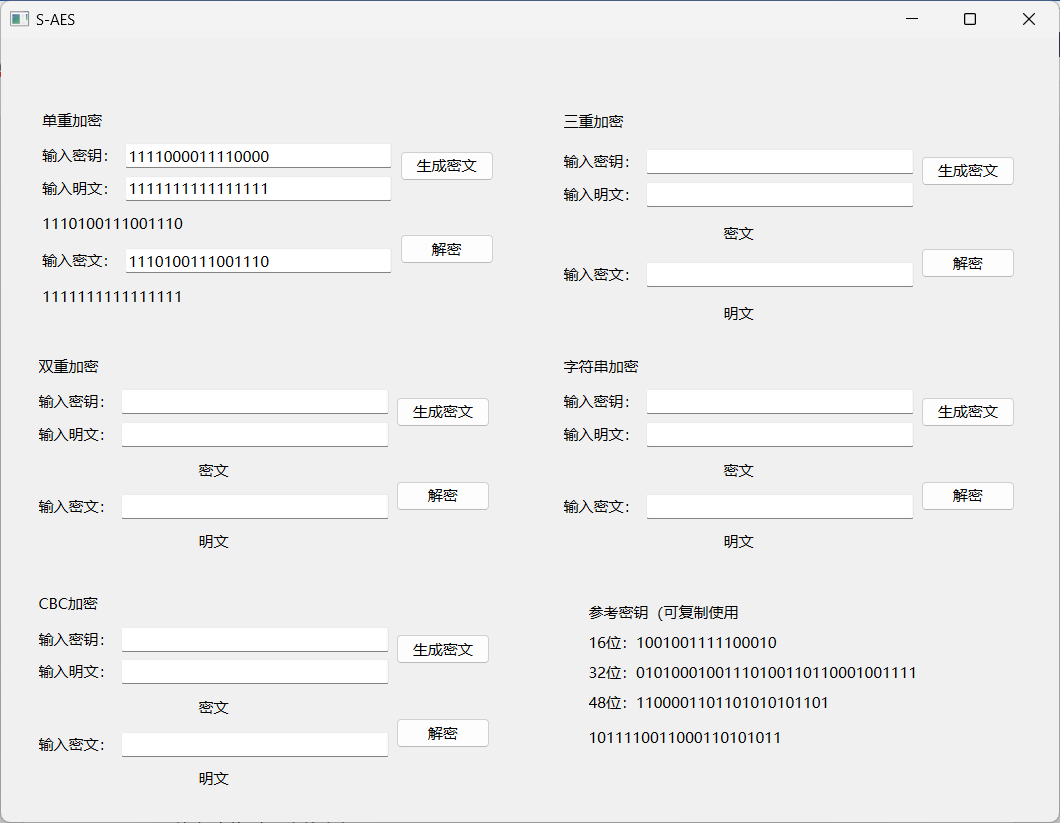


第二关 交叉测试

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。

我们组



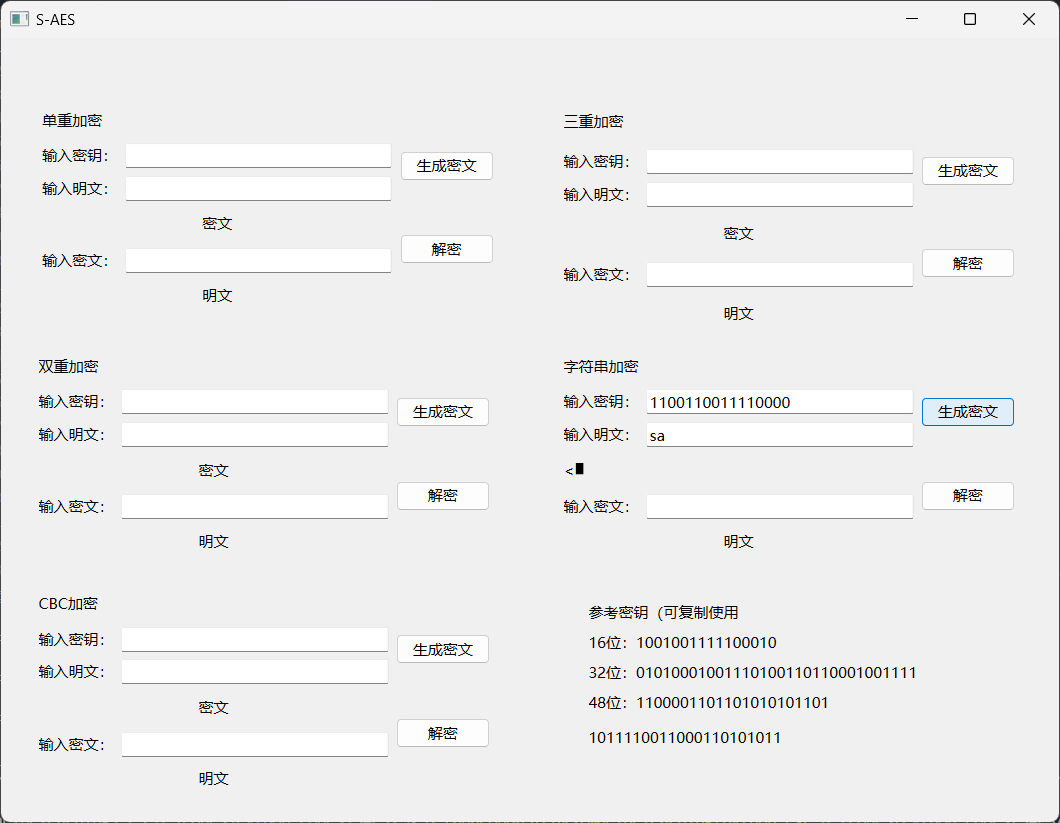
其他组

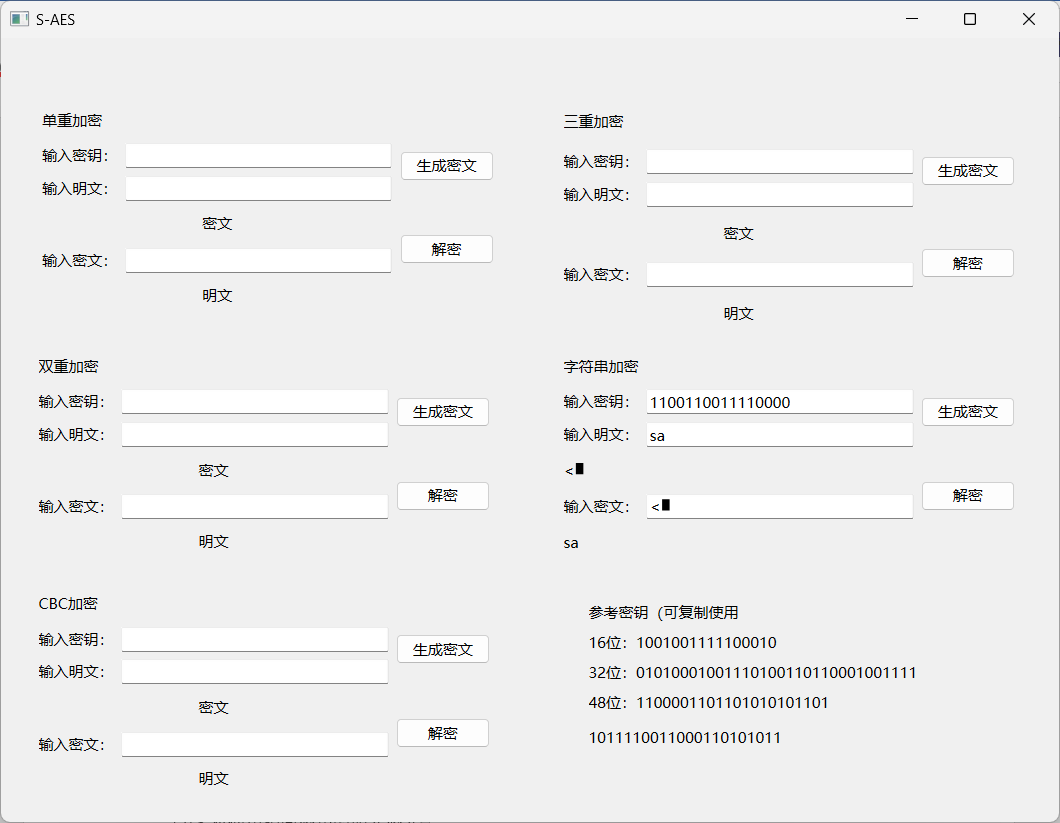
第三关 拓展功能

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)。

输入是ASII编码字符串



输出是ASII编码字符串

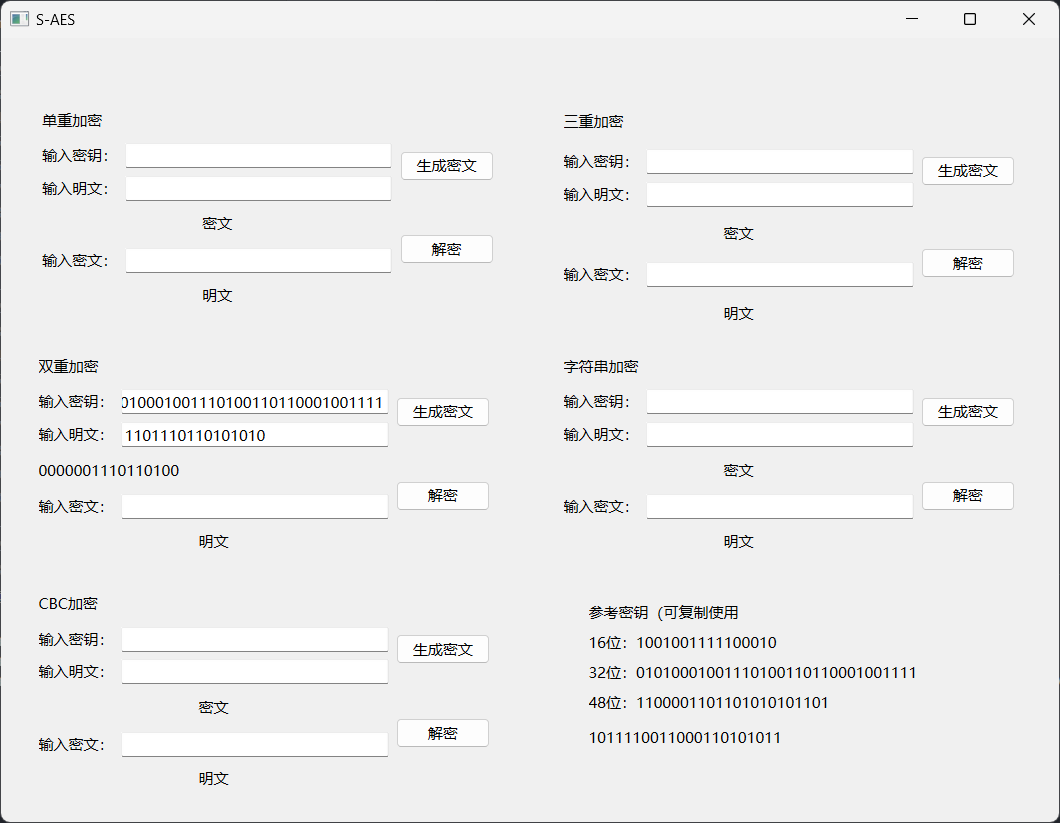


第四关 多重加密

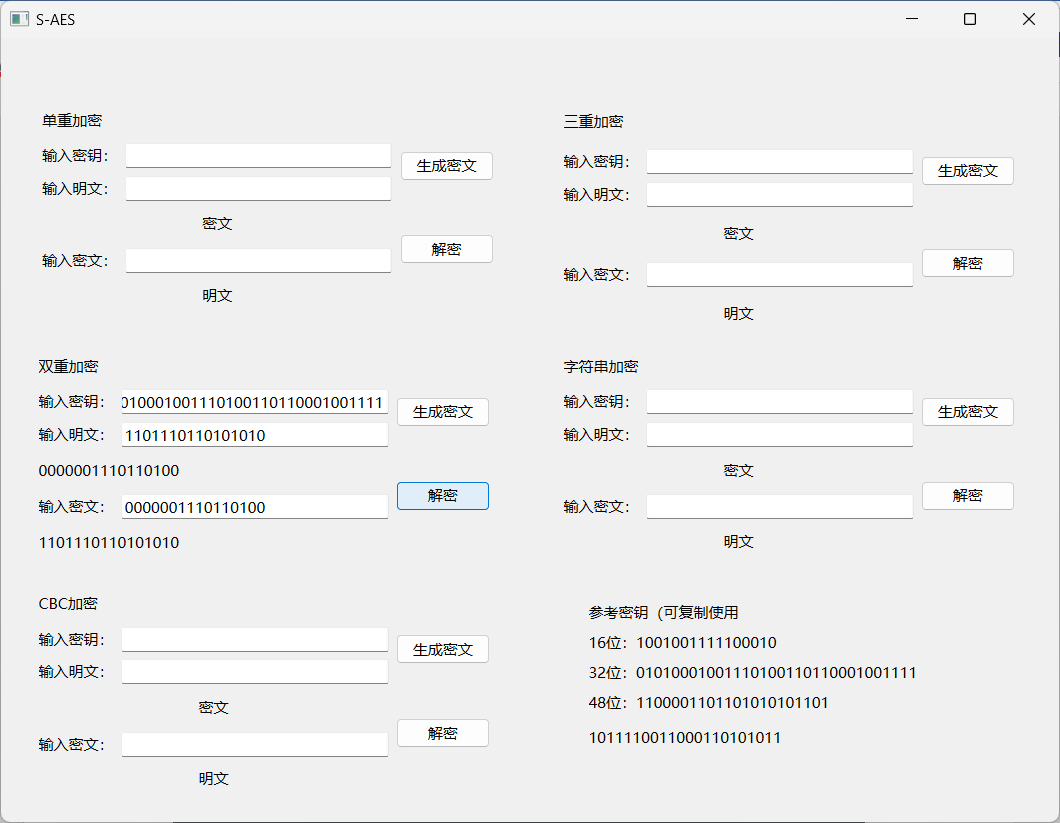
4.1双重加密

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

明文加密，这里用32bit的参考密钥



密文解密



4.2 中间相遇攻击

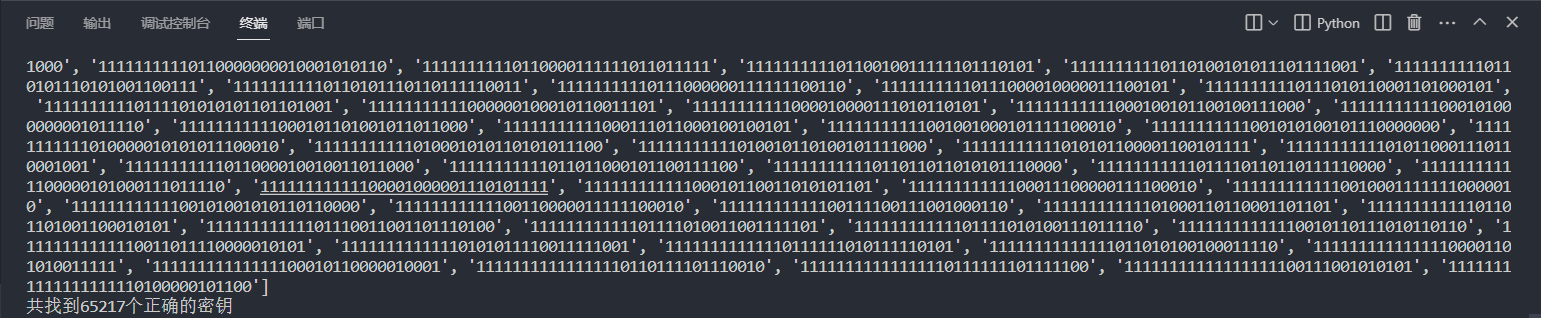
假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用中间相遇攻击的方法找到正确的密钥Key(K1+K2)。

（1）一对使用相同密钥的明文密文

k = "11100001101010011100001110100101"

p = '1011001110100100'

c = '0011100000101010'



共找到65217个正确的密钥

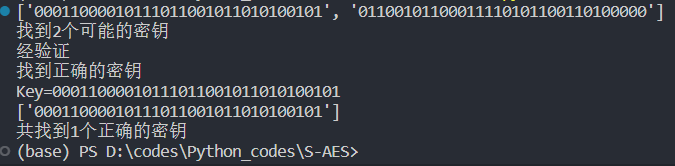
(2)多对使用相同密钥的明文密文

这里使用三对明文密文，它们使用相同的密钥

k = "00011000010111011001011010100101"

p = ['1100110011110000', '1111111111111111', '0000000000000000']

c = ['0001111011000001', '1110011110110000', '1110011010001010']

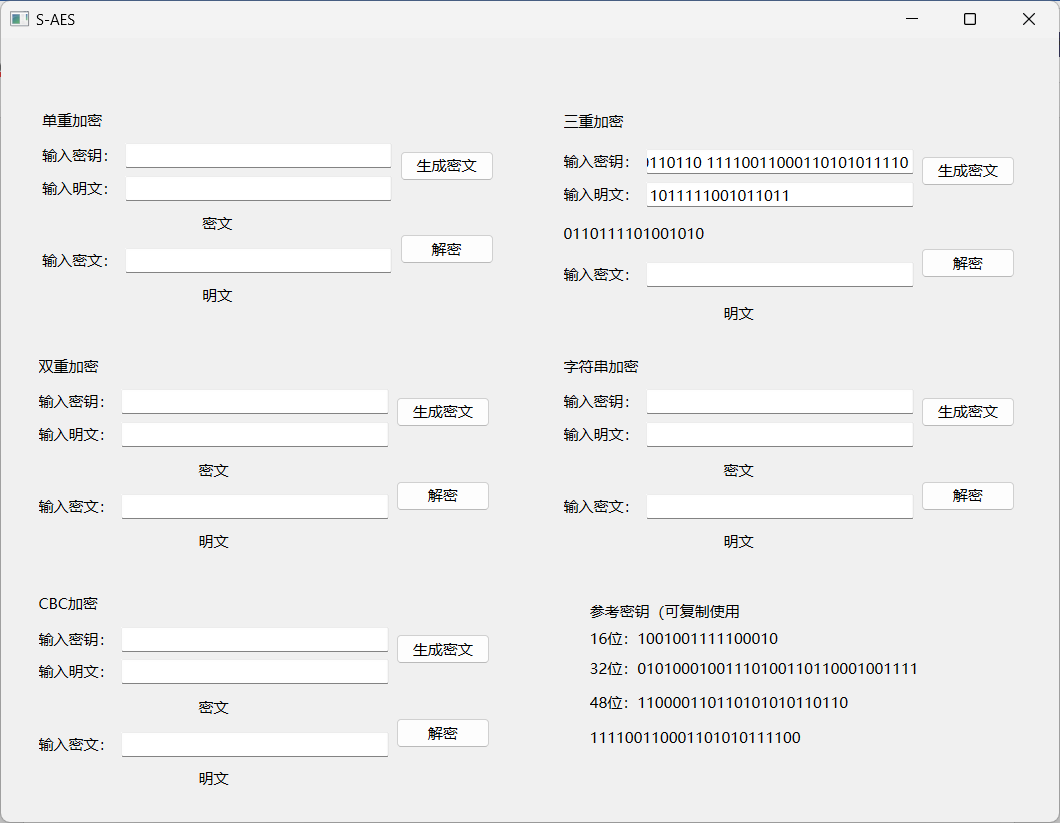


找到两个可能的密钥，经过验证后找到1个正确的密钥

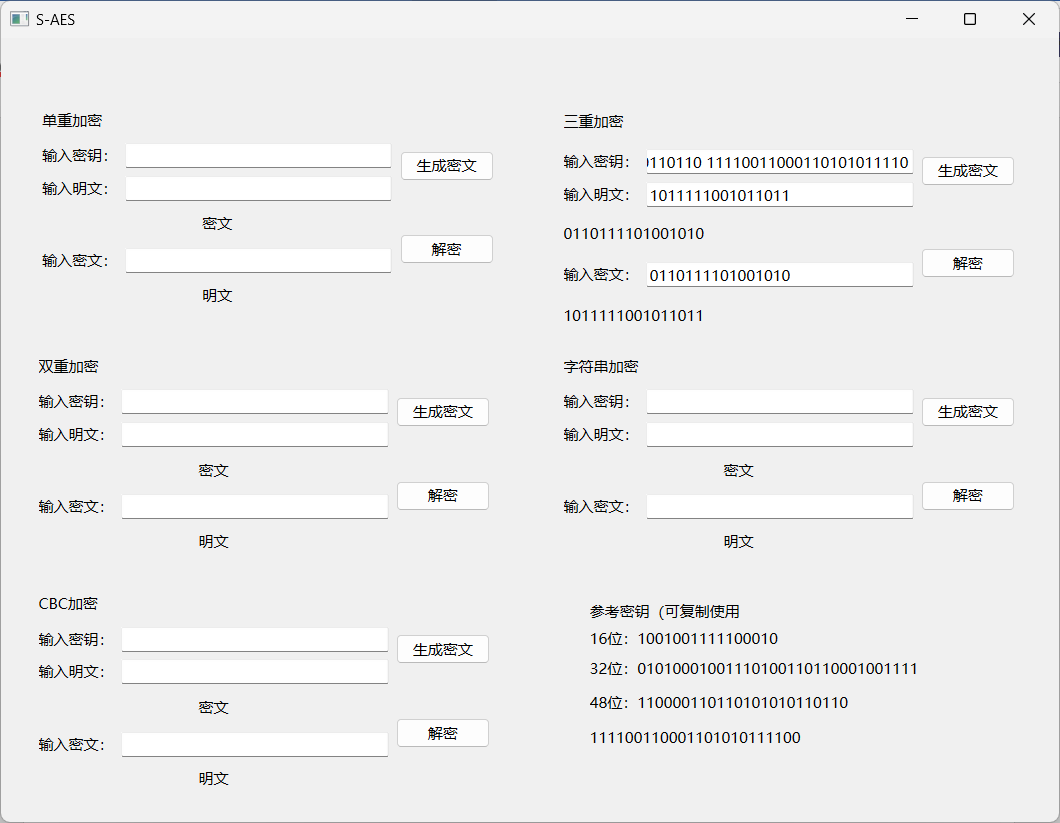
4.3三重加密

将S-AES算法通过三重加密进行扩展，使用48bits(K1+K2+K3)的模式进行三重加解密

明文加密，用48bit的参考密钥



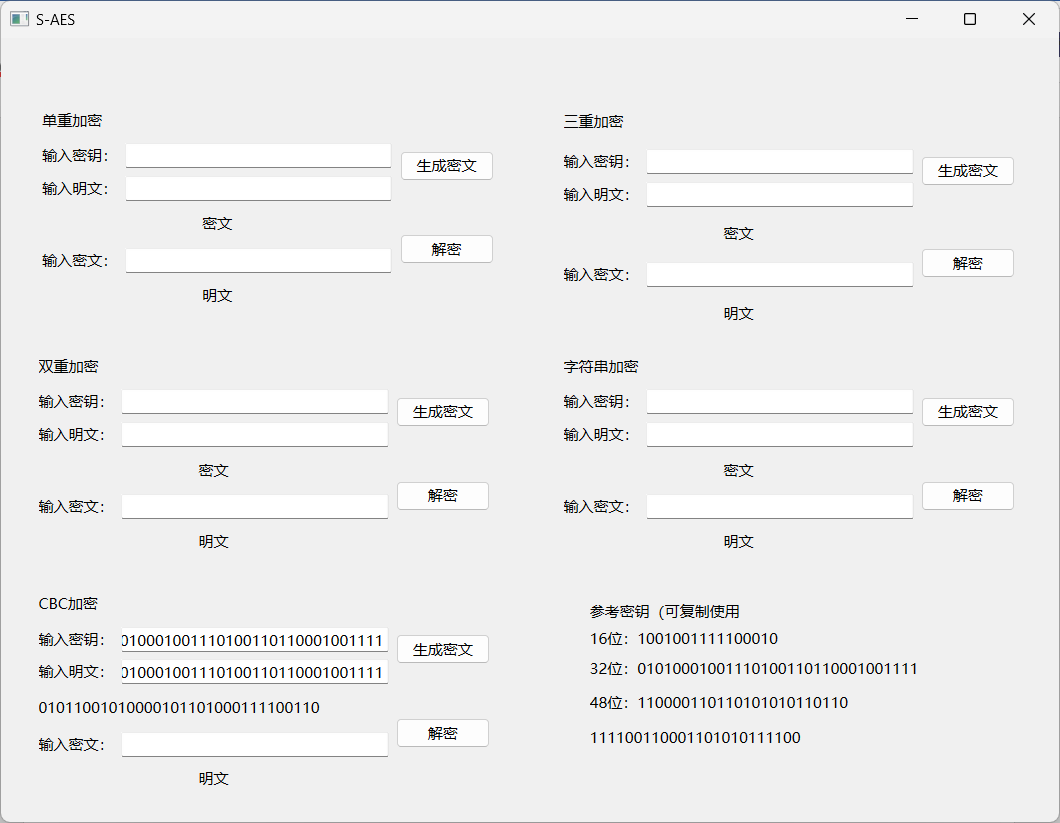
密文解密

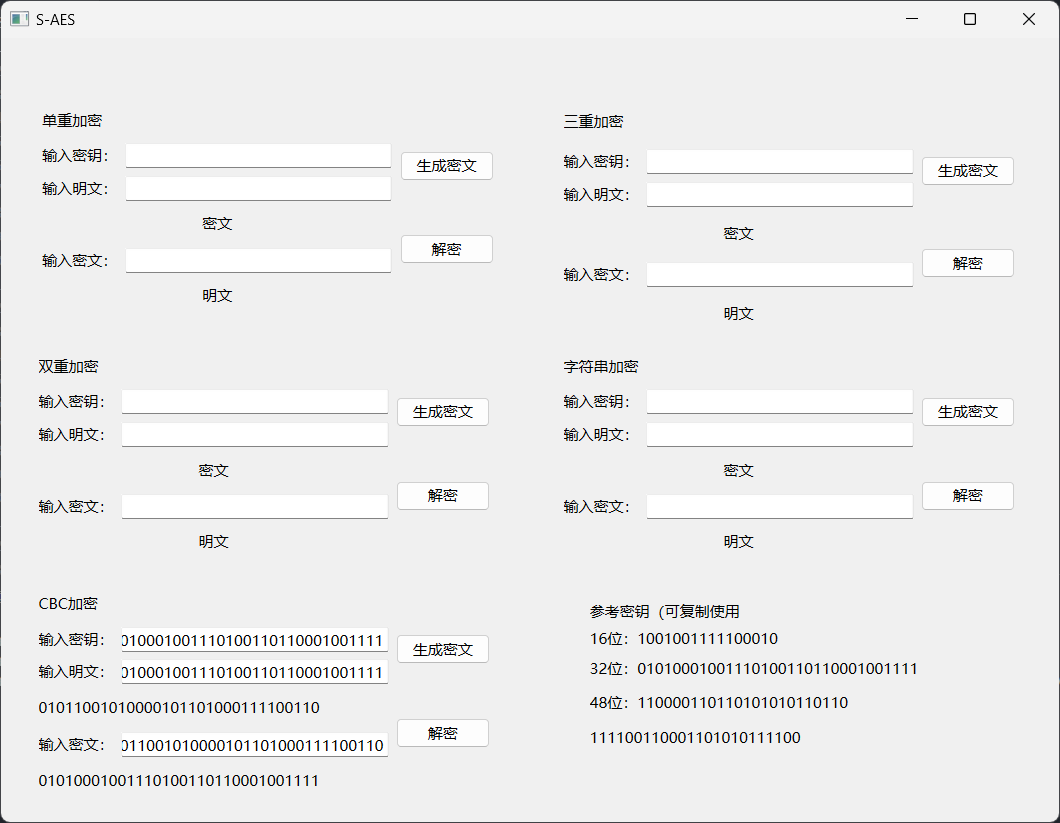


第五关 工作模式

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。





上图中明文和密钥均为“01010001001110100110110001001111”，下图为CBC对比篡改密文前后的解密结果。

