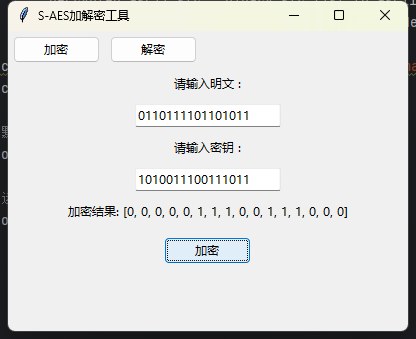
**第1关：基本测试**

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。

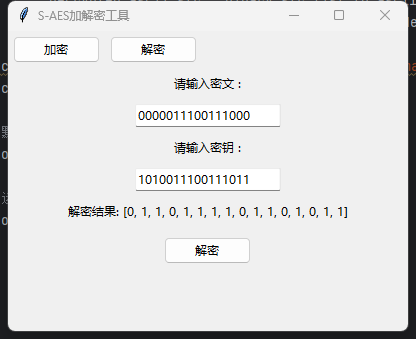
**1. 1 加密算法测试结果**



获得加密结果 0000 0111 0011 1000

**1.2 解密算法的测试结果**

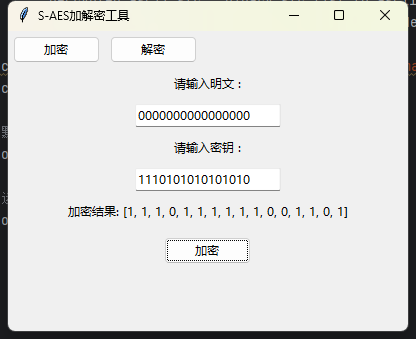
输入 密文 0000 0111 0011 1000 和 密钥 1010 0111 0011 1011



获得解密 1010 0111 0011 1011

**第2关：交叉测试**

和其他小组使用相同的密钥对相同的明文进行加密，得到相同的密文



**第3关：扩展功能**

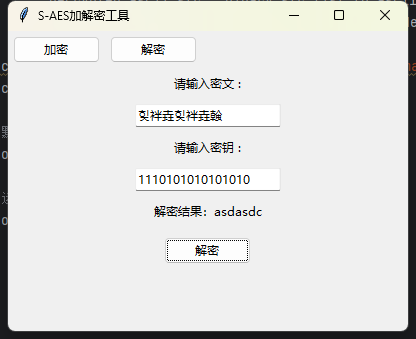
**3.1 ASII加解密**

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1 Byte)，对应地输出也可以是ACII字符串(很可能是乱码)。

**3.1.1 加密算法测试结果**



**3.1.2 解密算法测试结果**

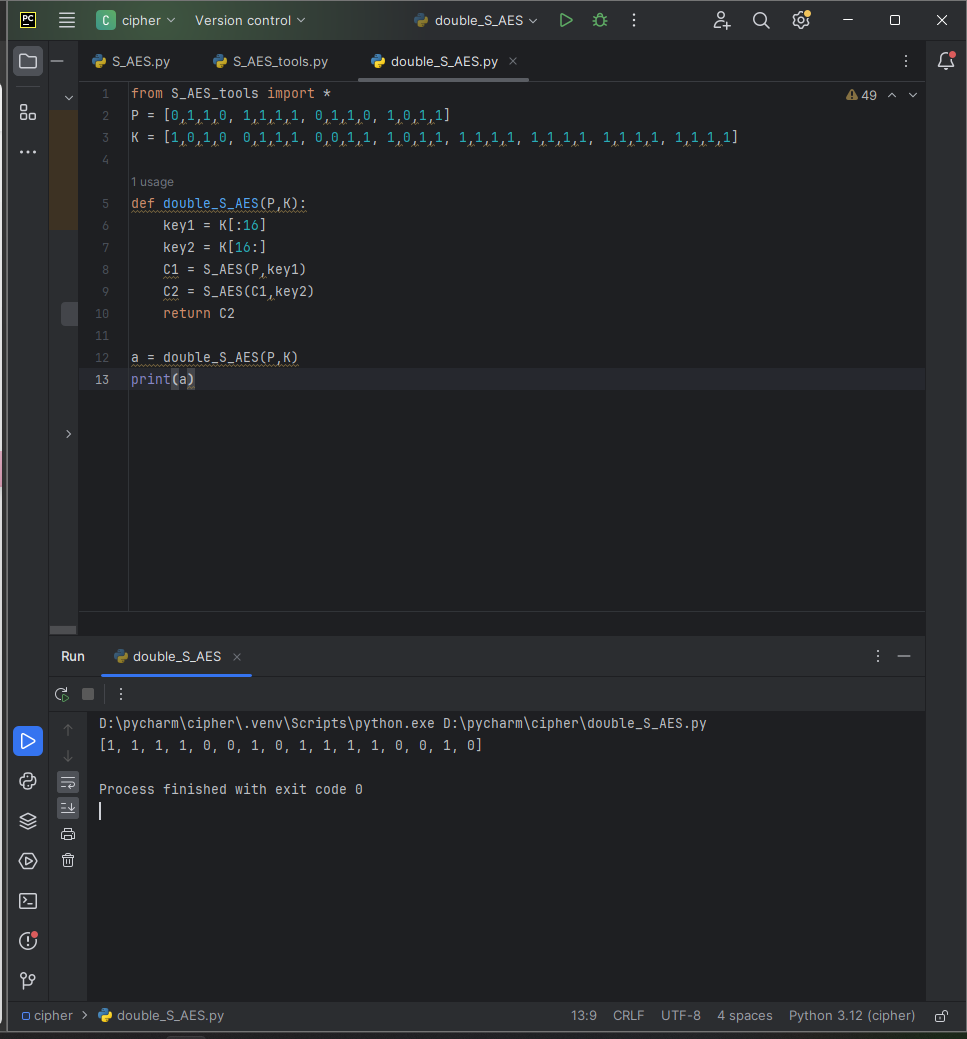


**第4关：多重加密**

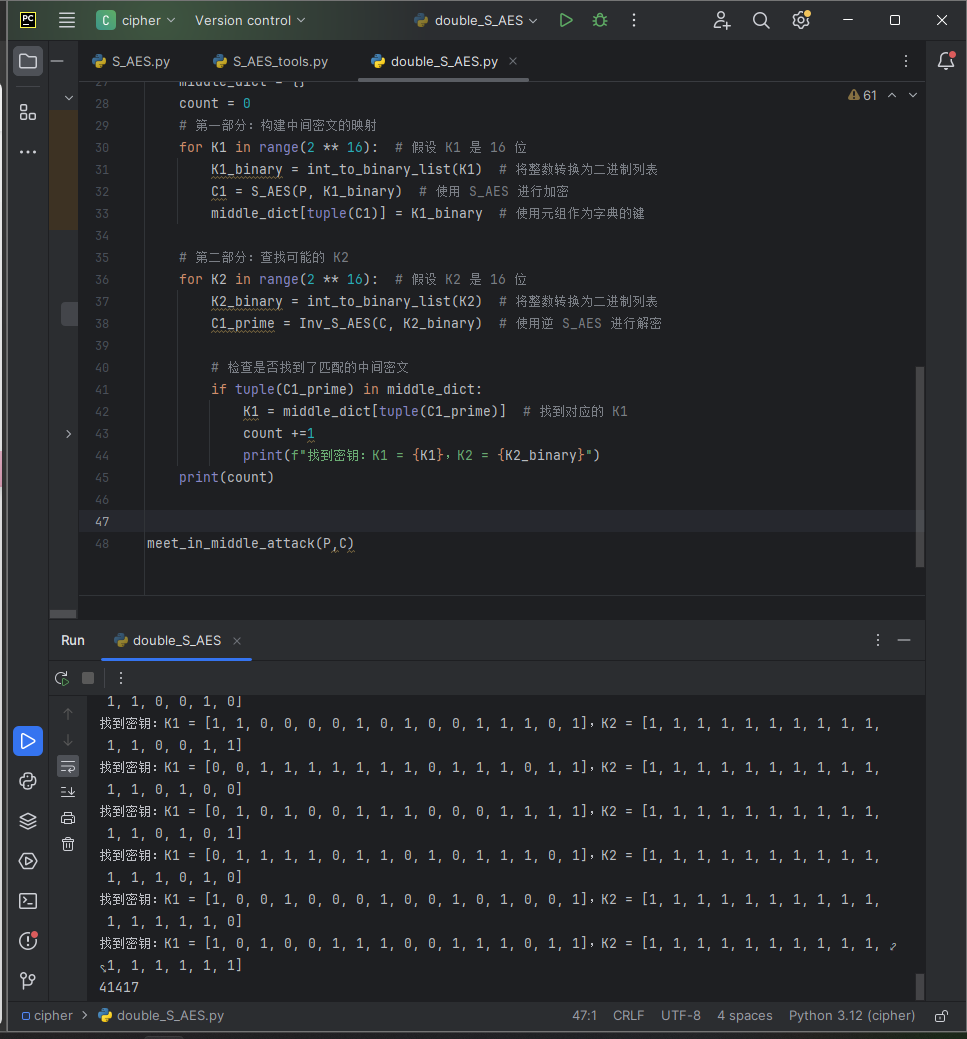
**4.1 双重加密**

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。

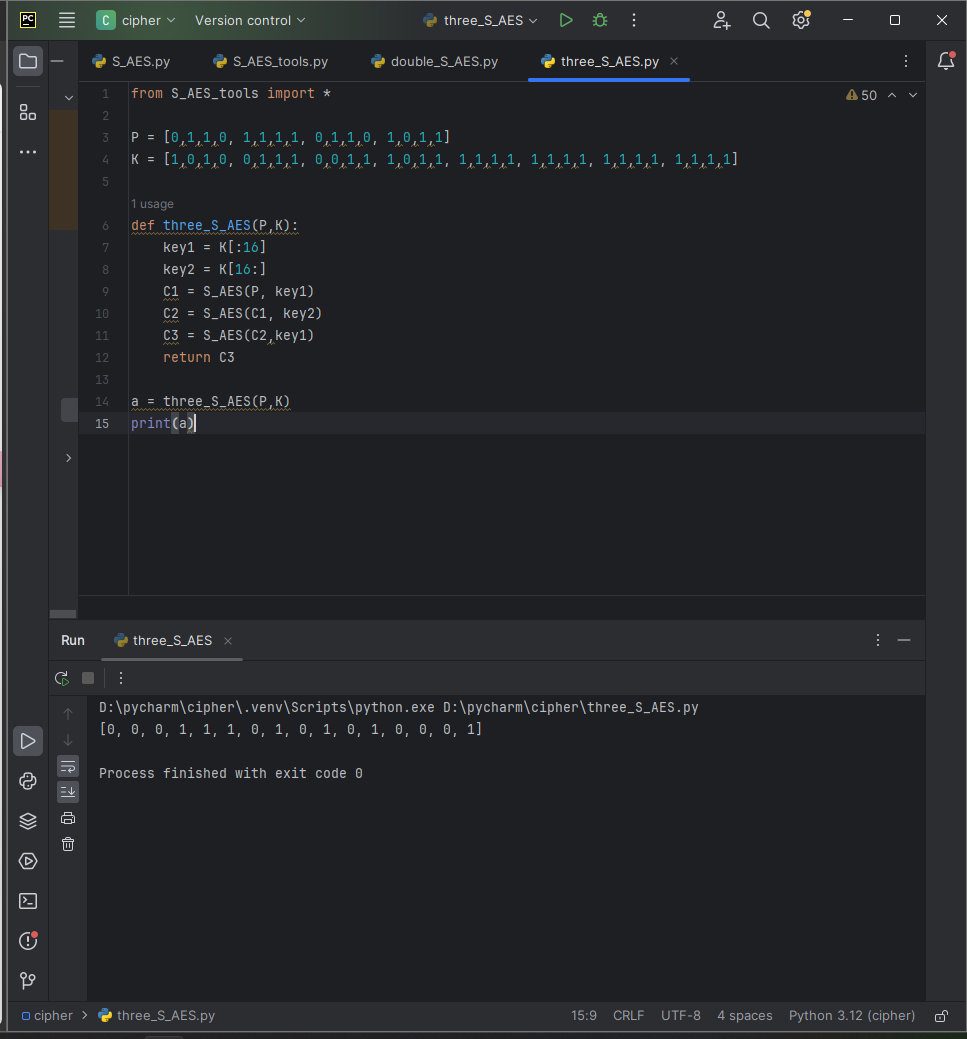
**4.1.1 加密算法测试结果**



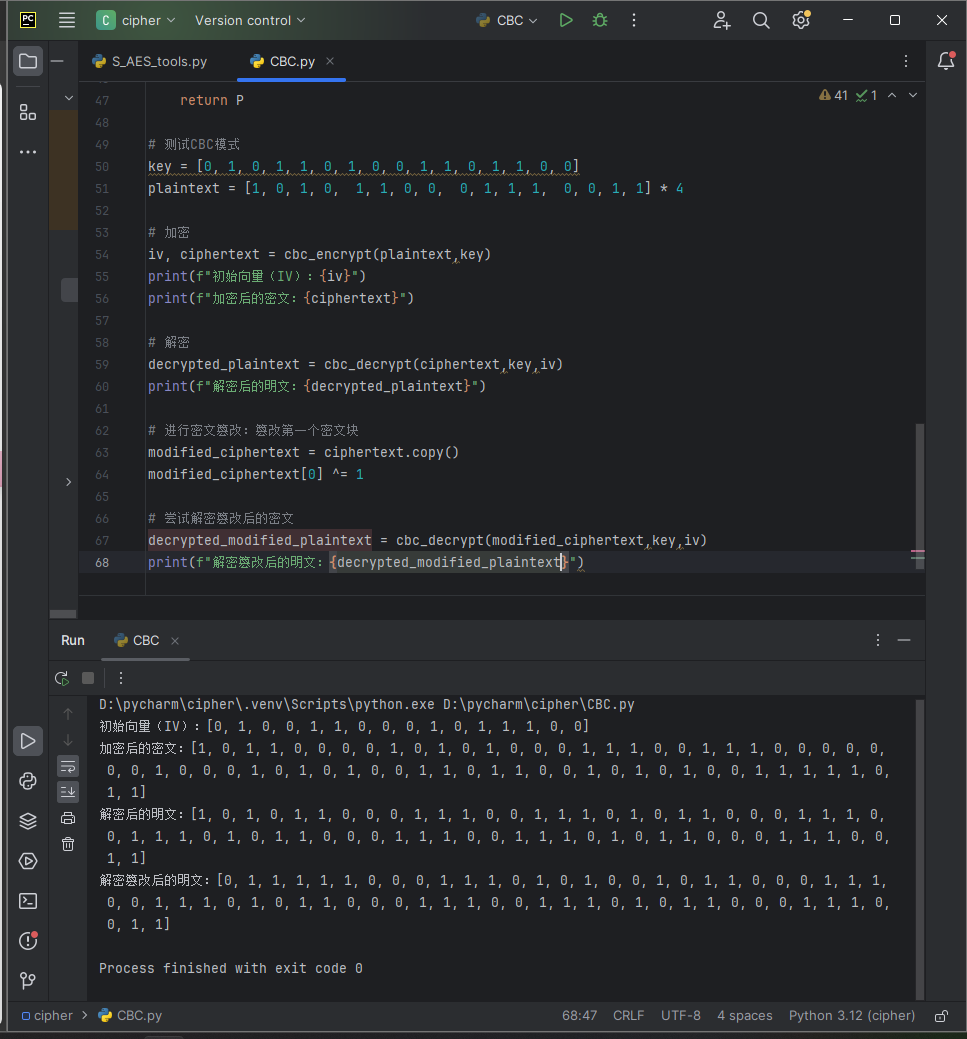
**4.2 中间相遇攻击**



**4.3 三重加密**



**第5关：工作模式**



由于篡改，解密后的明文将发生变化，展示了 CBC 模式对密文篡改的敏感性。