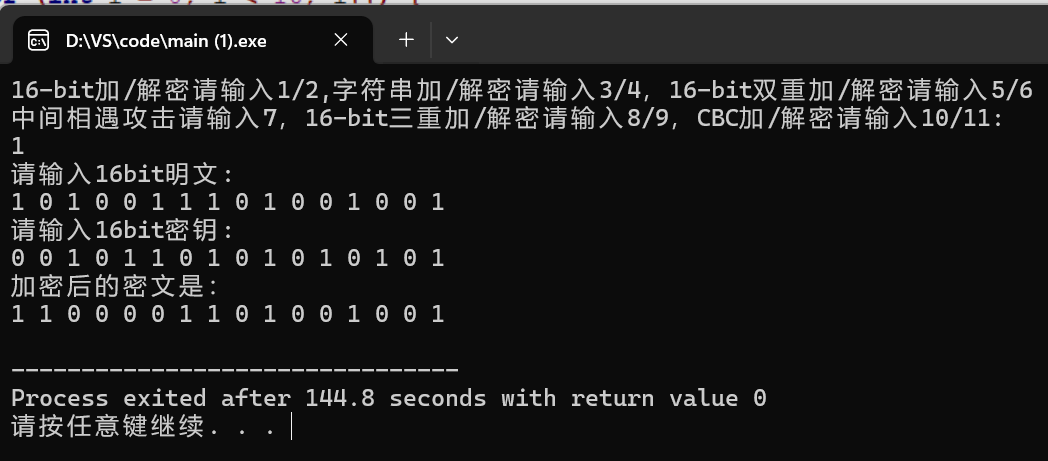
**测试结果**

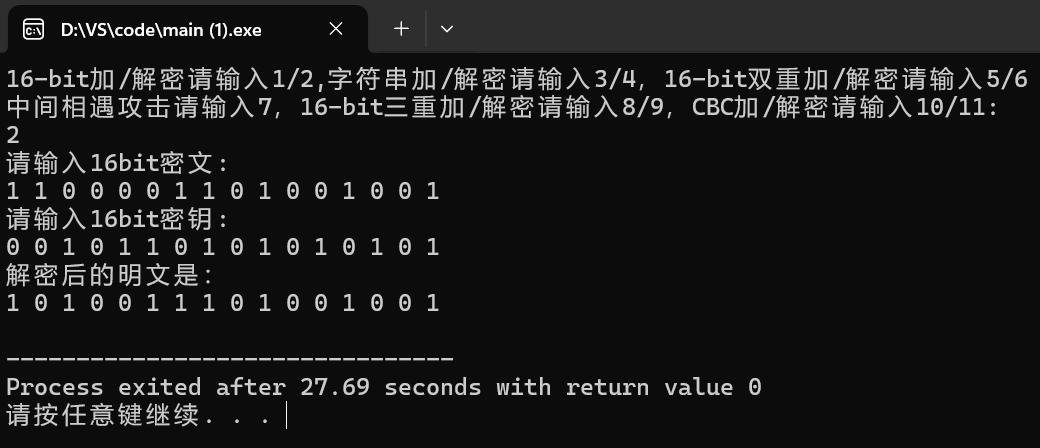
1. **基本测试**

已实现S-AES的基本功能以及加解密一体，输入16bit的数据和16bit的密钥，输出是16bit的密文。

加密：

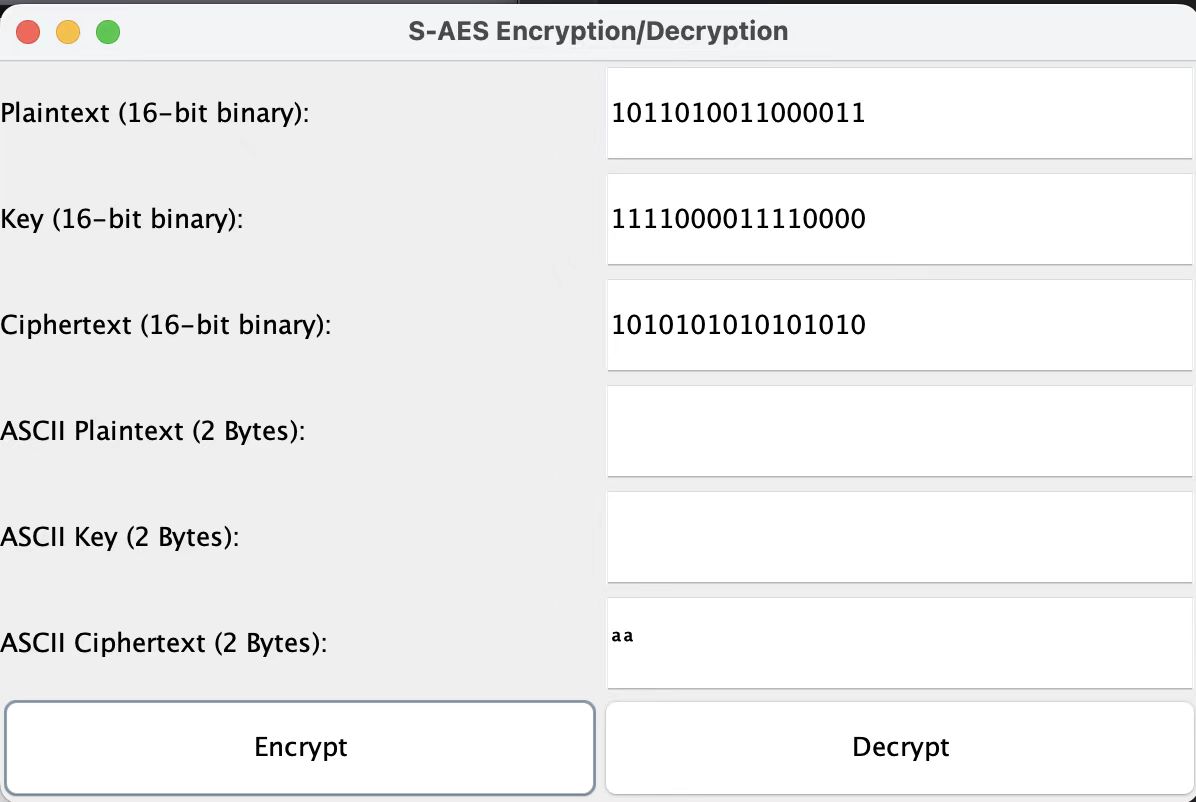


解密：

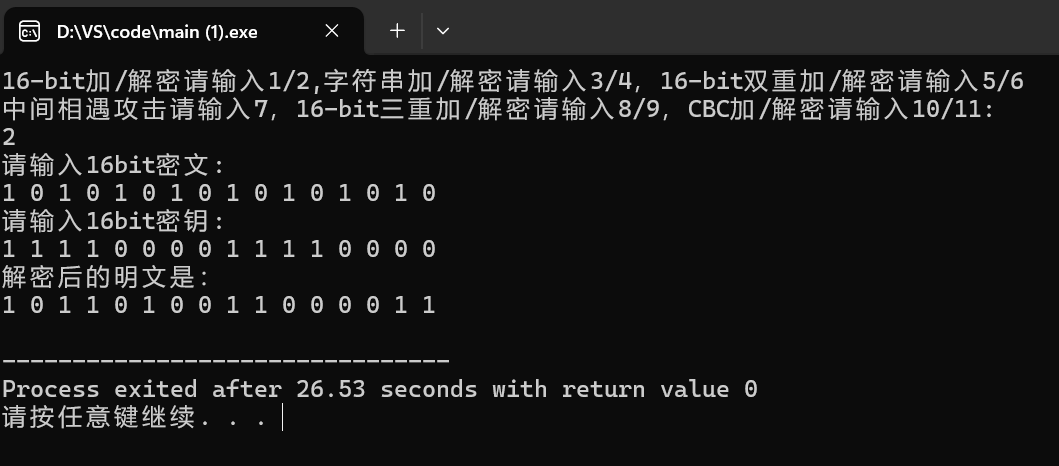


1. **交叉测试**

查找到某组的明/密文对以及对应密钥如下：



将该明文以及密钥输入，得到的密文结果如下：

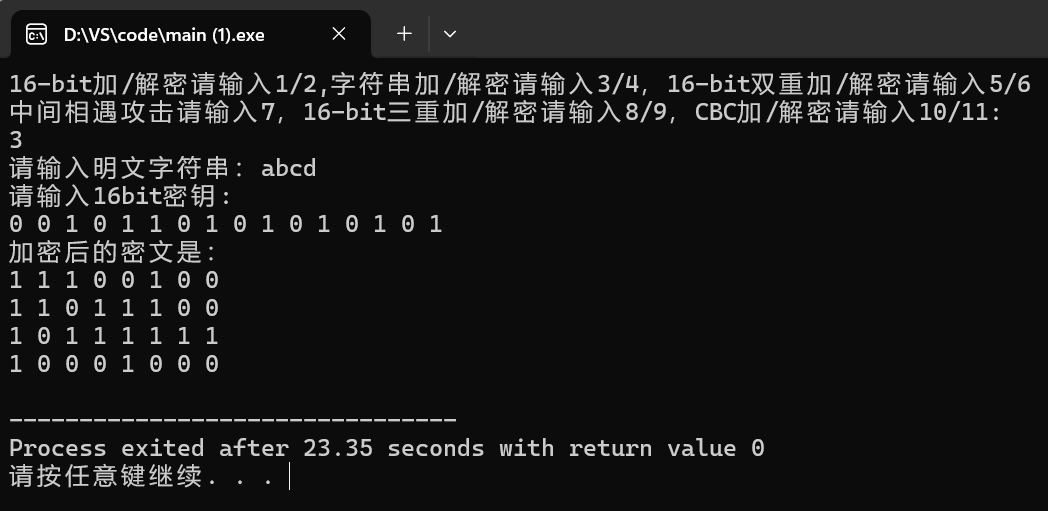


该结果与上图一致，测试通过。

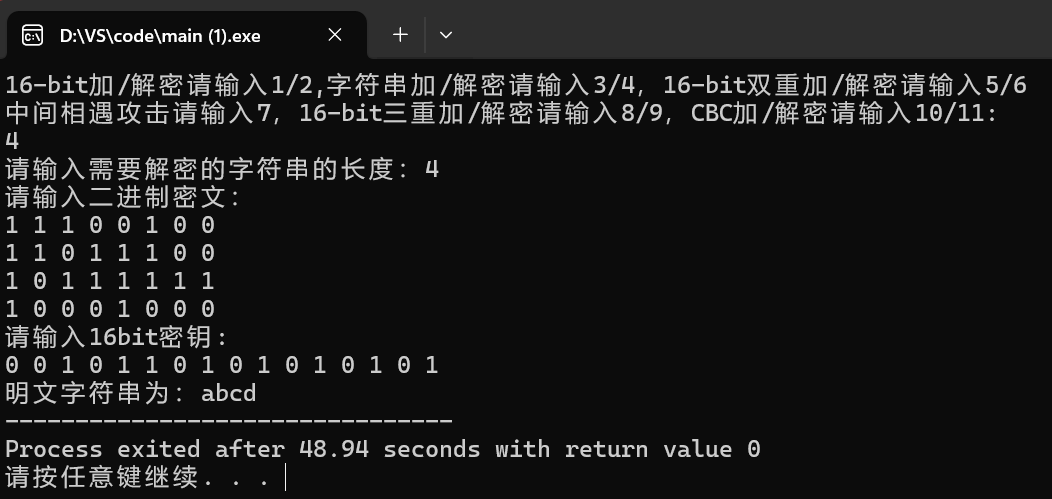
1. **扩展功能**

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，字符串长度不限，但要为偶数。将每个字符进行加密后，每个字符对应输出为8bit的密文；进行解密时，输入所有密文，输出对应的字符串。

（1）加密：



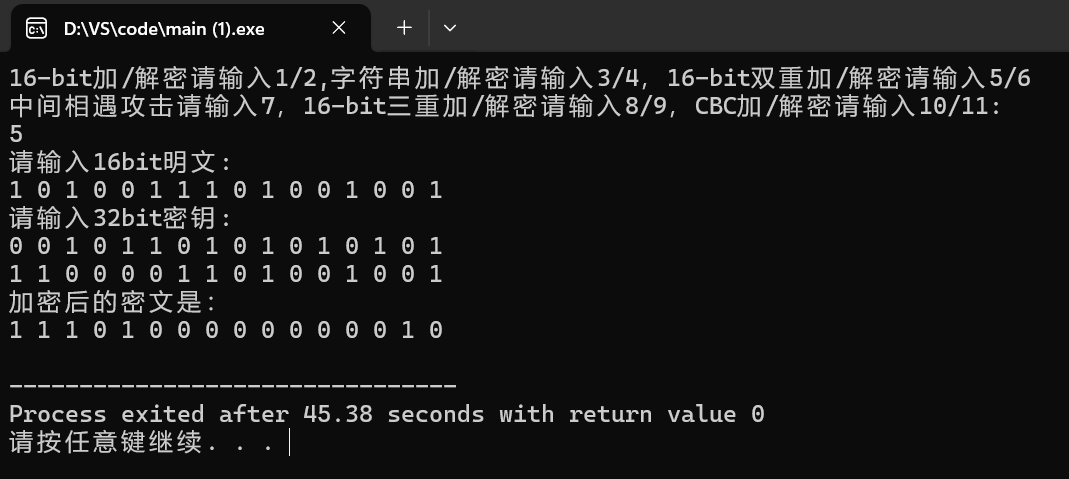
（2）解密：



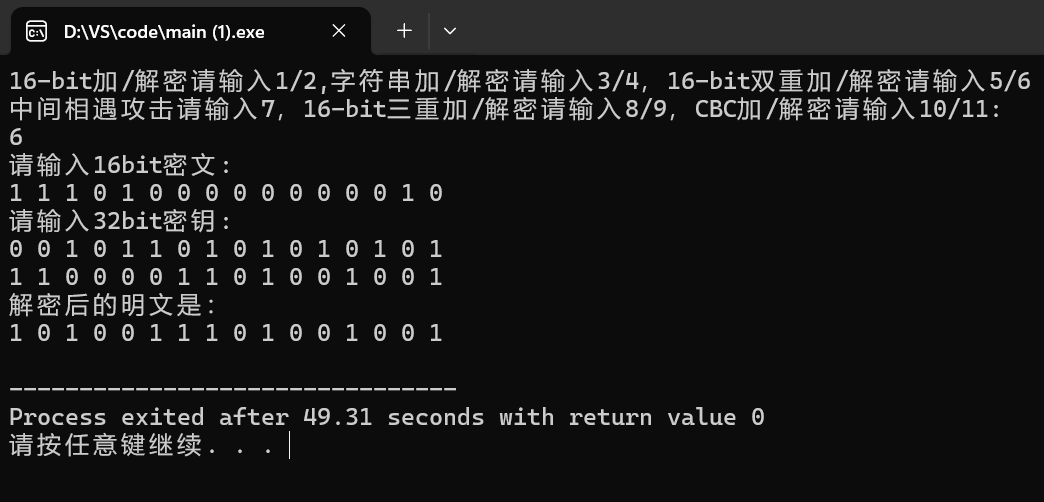
1. **双重加解密**

将S-AES算法通过双重加密进行扩展，分组长度仍为16bit，但密钥长度为32bit。KEY（KEY1+KEY2）

加密：

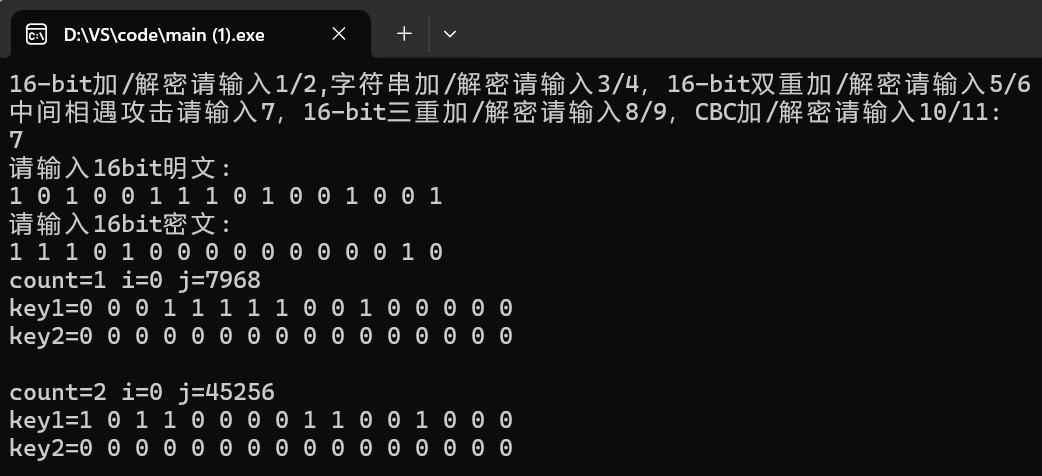


解密：

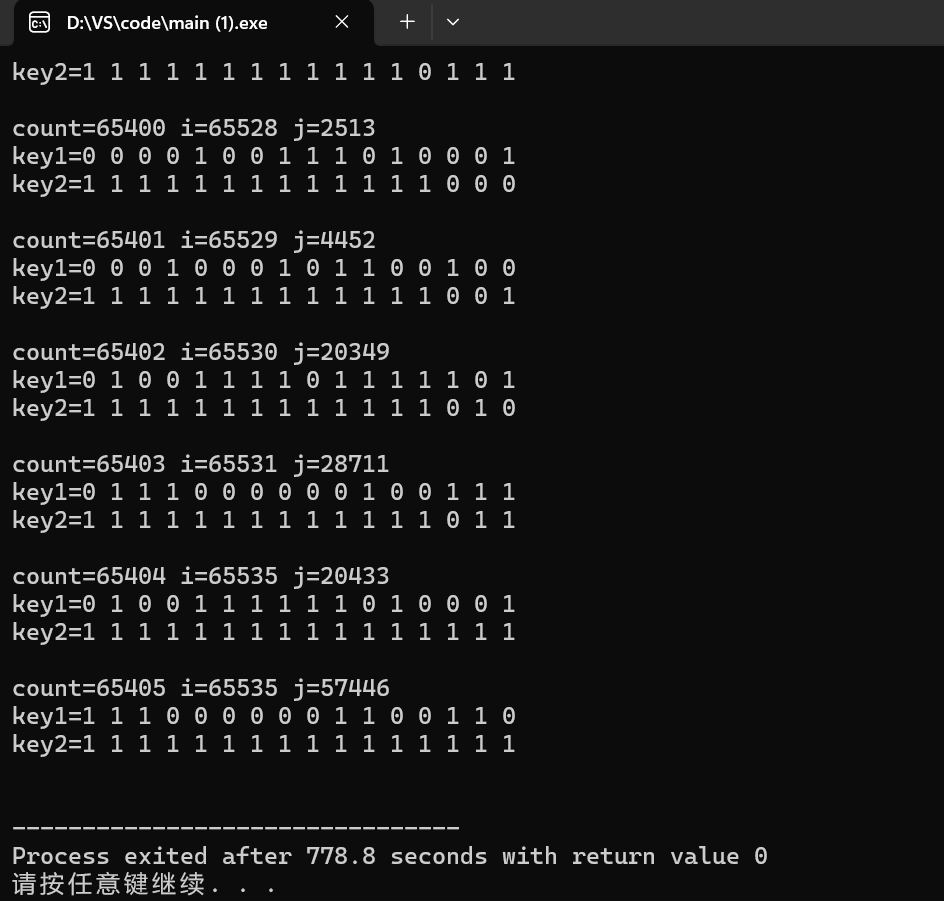


**五、中间相遇攻击**

输入一对明密文对，将所有可能的密钥对输出。

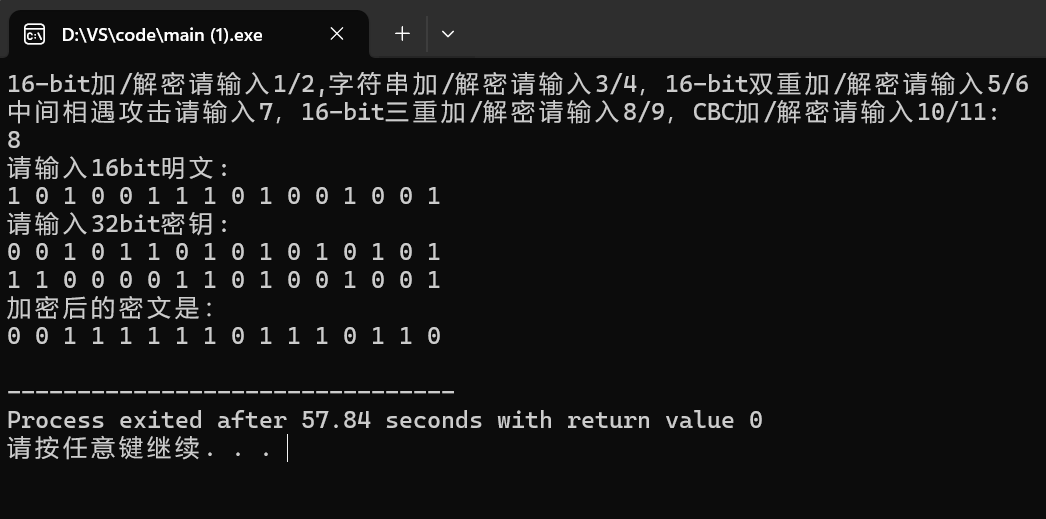


结果：

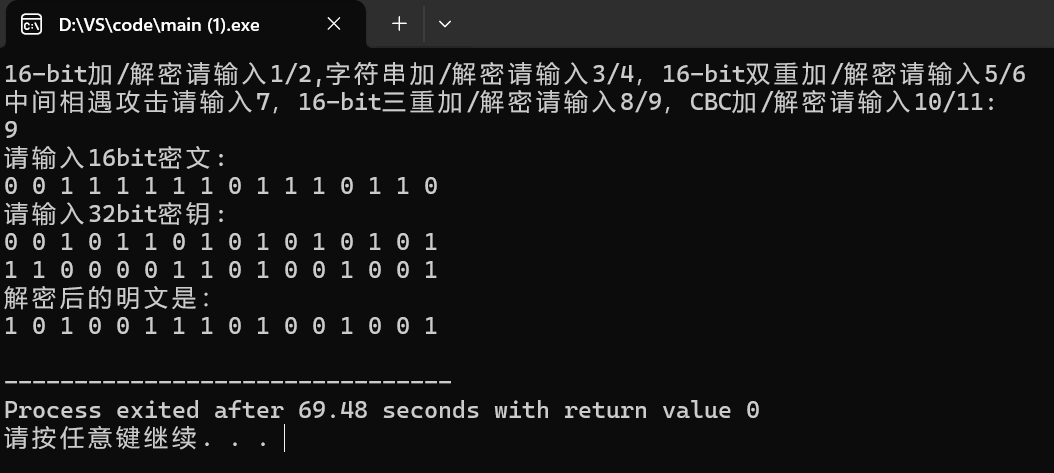


**六、三重加解密**

将S-AES算法通过三重加密进行扩展，使用32bit密钥的模式进行三重加密解密

加密：

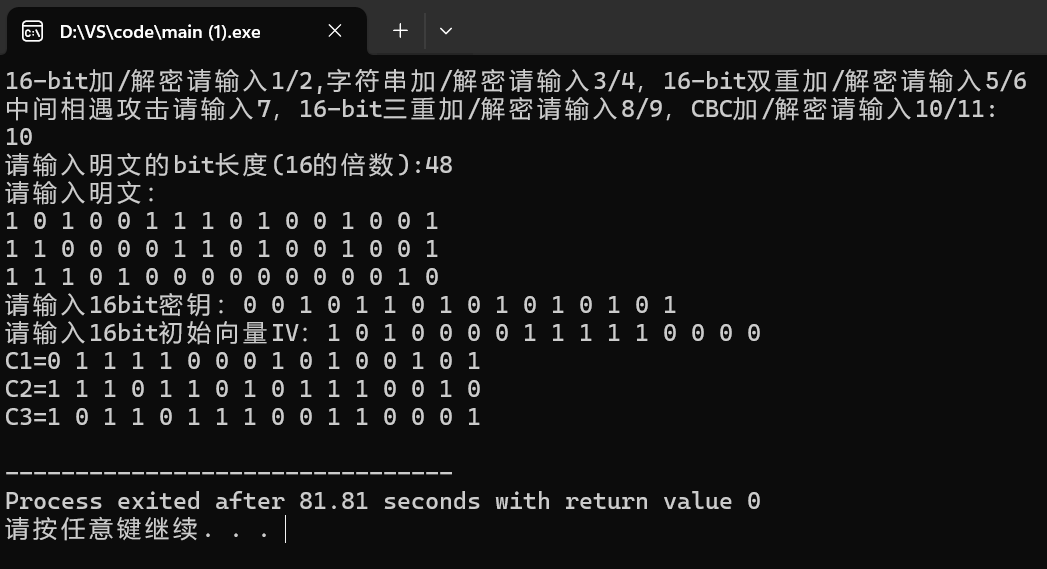
解密：



**七、工作模式CBC**

基于S-AES算法，使用密码分组链模式对较长的明文信息进行加解密。

加密：



解密：

