实验二：编程实现DES的CBC模式

# 实验要求

在本项目中，我们将在 CBC（密码分组链接）模式下使用 DES 对文件进行加密和解密。“tempdes.c”是用于加密/解密固定的 64 位块的核心文件。在本作业中，您需要通过实现 DES-CBC 操作模式，扩展此框架代码以获取任意大小的输入文件并对其进行加密/解密。实际上，您必须实现 CBC 模式，并且除了 tempdes.c中的功能外，不允许使用任何内置功能。您可以在您的课本中找到有关 DES-CBC

的信息。

可以通过对照输入文件“test.txt”检查您的工作。如果您正确实现了算法，则应该在“test.des”中获得输出。

**要求**

a. 只需使用 tempdes.c 中出现的内置函数

b. 您的代码应生成以下形式的可执行文件：

./tempdes iv key inputfile outputfile

参数说明如下：

-iv：要使用的实际iv：必须表示为仅由十六进制数字组成的字符串。

-key：要使用的实际密钥：它必须表示为仅由十六进制数字组成的字符串。

-inputfile：输入文件名

-outputfile：输出文件名

示例：

./tempdes fecdba9876543210 0123456789abcdef test.txt test.des

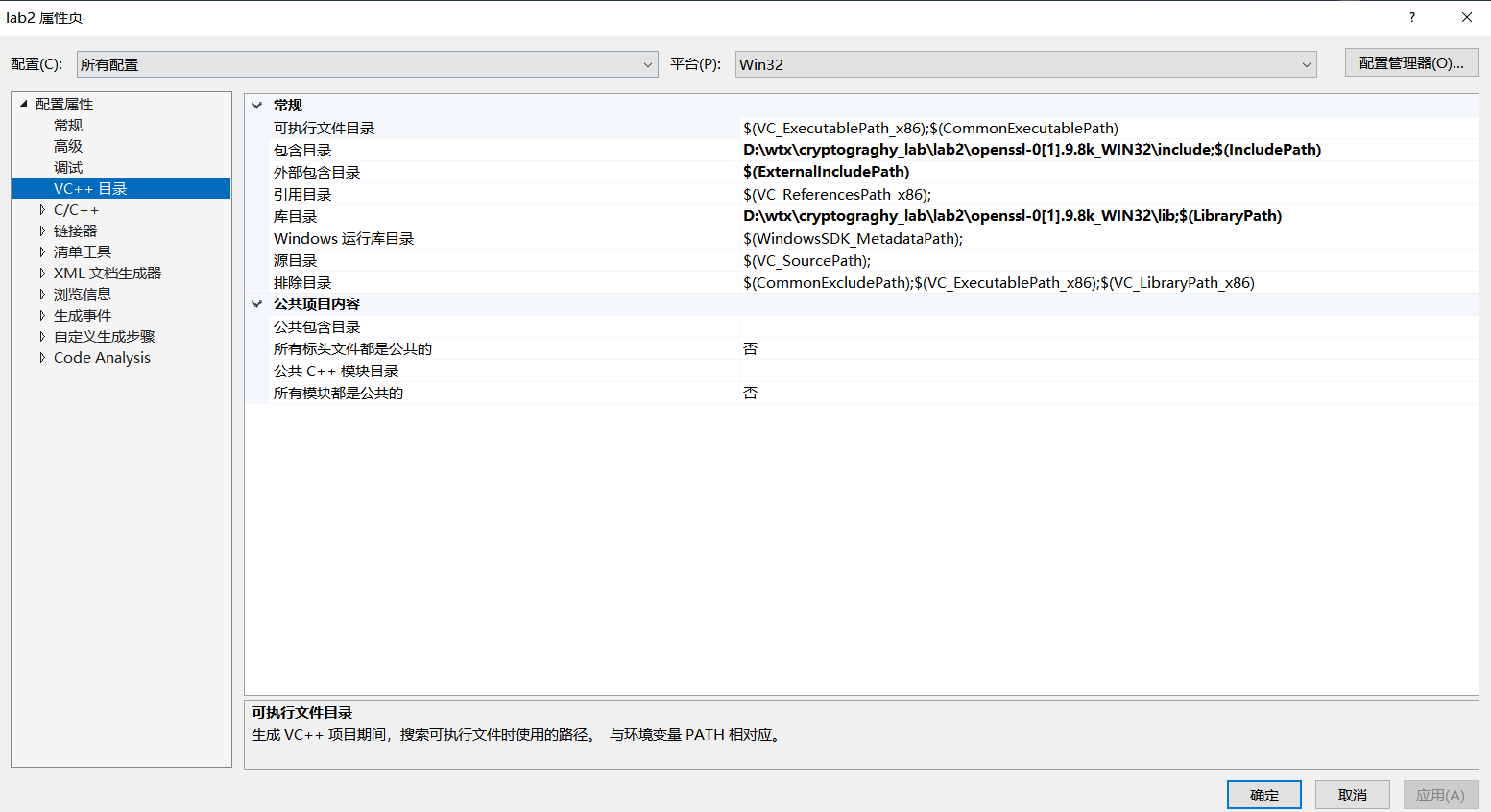
如果存在无效的参数，代码应向用户返回适当的消息。请务必考虑密钥无效的这种情况。

# 实验环境

Windows 10 + vs2022 + openssl 1.0

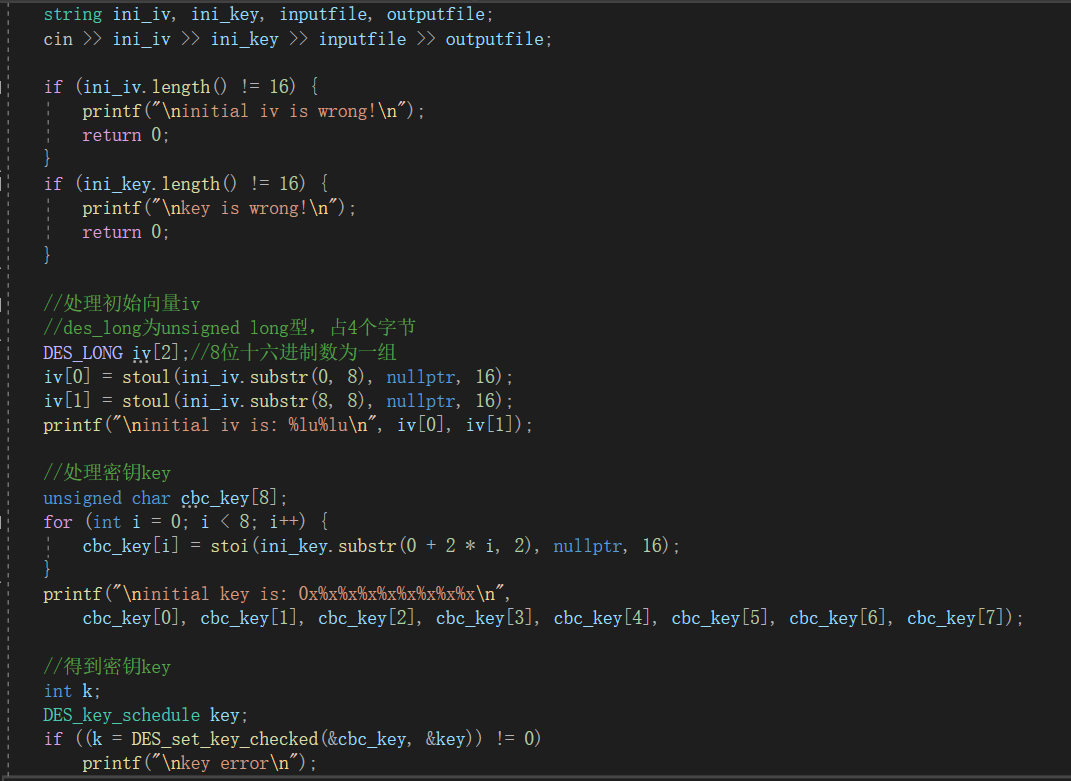
# 实验准备

**配置vs项目**

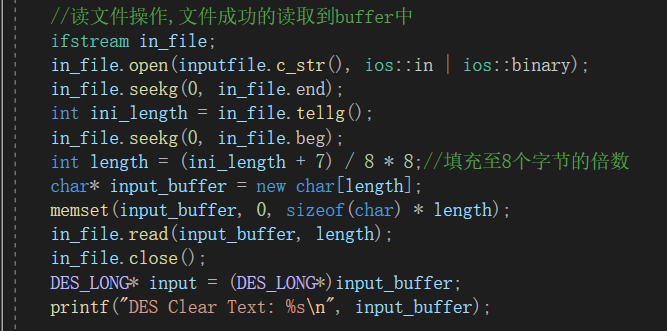


# 实验内容

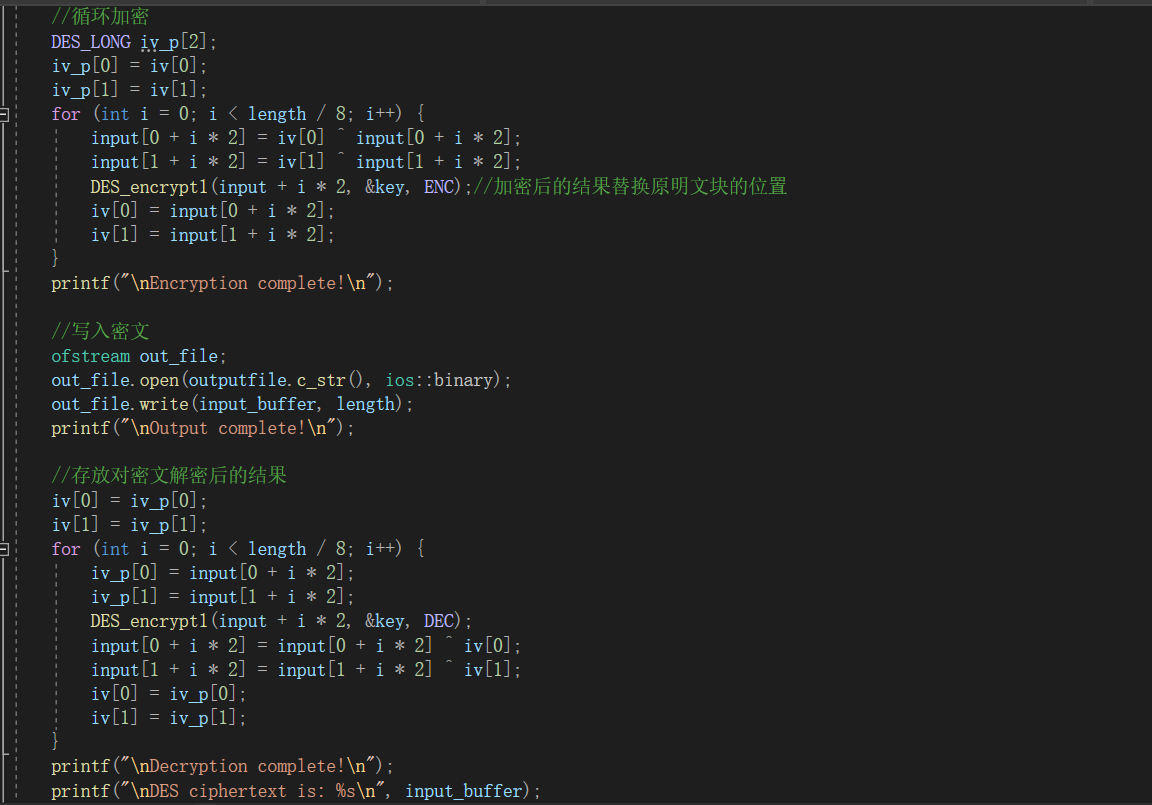
处理iv和key，并判断是否满足条件：iv和key为16位十六进制数；且key正确



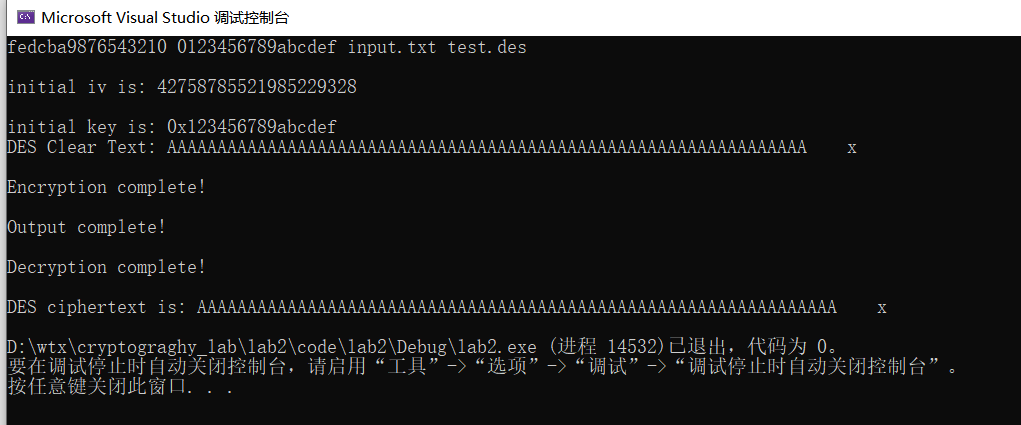
获得明文并进行处理



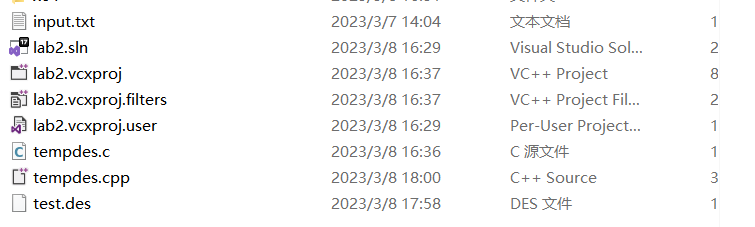
对明文进行加密，并对密文进行解密



# 实验结果



明文与密文解密后的结果相同



产生了test.des文件