**实验四 AES-CBC/AES-CTR加密算法**

**姓名：\_\_ 胡 聪 \_学号：\_\_\_\_\_ 180110505 \_\_\_**

1. **（必做）运行截图**

*文本

描述已自动生成CBC*

***文本

描述已自动生成****CTR*

1. **（选做）总结**

*对AES-CBC和AES-CTR算法的理解，实验过程总结、感受、建议等等。*

**CBC的加密过程：先将plaintext填充为16字节的整数倍，然后将plaintext等分为n份。第一次加密时，将IV与P1进行异或操作得到结果，然后将这个结果进行AES加密，得到C1。将C1链接到密文中去，并将C1代替IV,参与下一次的异或操作。然后重复上述操作，直到所有的block都进行加密。**

**CBC的解密过程：**

**选取密文的前16个字节，这16个字节就是IV。然后将去除IV的plaintext等分为n份。先取出C1(第一块密文)，将C1通过AES解密得到结果T1, 然后将T1与IV异或的得到第一块明文。再用C1替换IV参与下一次解密运算，重复上述操作。**

**CTR的加密过程：**

**先选取counter,如果没有16字节就填充，现将counter通过AES进行加密，得到结果T1,然后将T1与明文的第一分组进行异或得到结果C1,将C1链接到密文上，然后将counter+1进行下一轮加密。**

**CTR的解密过程：**

**选取密文中前16个字节作为counter,然后将去除counter的密文按照16个字节等分，最后一个非整16字节的单独处理。**