实验三 CBC和CTR模式下的AES

实验目的

- 了解分组密码的结构特点；
- 掌握传统分组密码结构AES，以及AES在两种工作模式CBC和CTR下的实现；
- 通过使用Python（推荐）或者C或者Java，编程分别实现CBC和CTR模式下的AES加密解密。

实验内容

- 在本次实验中，需要实现两个加密/解密系统，一个在密文分组链接模式（CBC）下使用AES，另一个在计数器模式（CTR）中使用AES；
- 完成程序后，使用附件的test.txt中给出的四组密钥和密文（十六进制形式）来验证你的代码。

实验时间与地点

- 4月16日晚上
- 思贤楼303机房

实验要求

- 在两种模式下，16字节的加密IV都要求是随机生成的，并被添加到密文前面；
- 对于CBC加密，要求使用PKCS5填充方案；
- 对于AES的基本实现，你可以使用现有的加密库，如PyCrypto（Python），Crypto++（C++）或任何其他语言和库；
- 要求自己实现CBC和CTR模式，而不是直接调用AES库的内置功能；
- 在线提交源码和实验报告；
- 实验报告需包括实验结果（四个密文的解密结果）、重要代码段解释以及本次实验总结；
- 实验代码禁止抄袭，可以在网上进行参考，但是如果没有任何改变，将判定抄袭，本次实验记0分；
- 鼓励大家思考新的求解方法和代码，对于能够用新思路求解出较好结果的同学本次实验加分的奖励；
- 实验报告截止时间为4月23日。

> 本次实验设立3个java小助教，2个C++小助教，4个python小助教，欢迎大家提前来找我们检查。