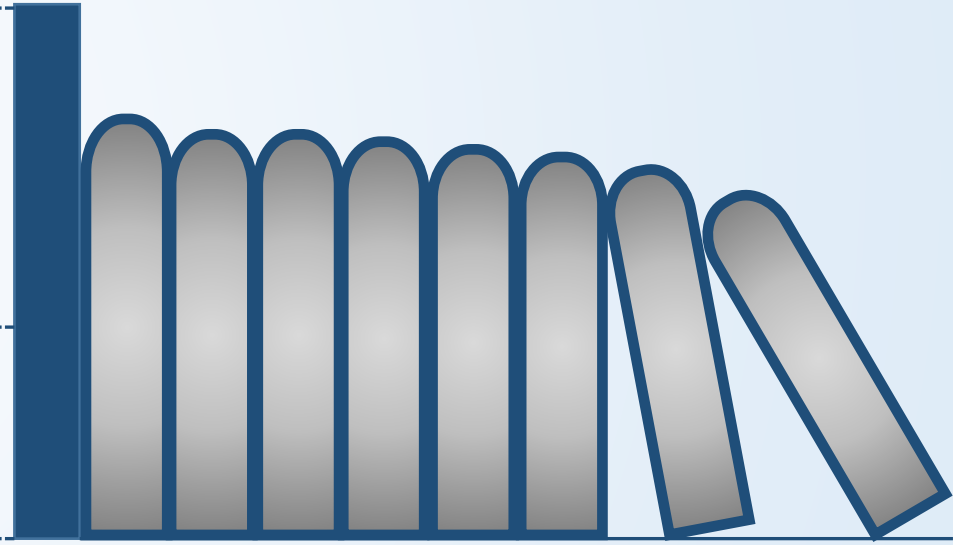
哈爾濱工業大學(深圳)
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

# 分组密码模式

主讲教师：蒋琳

实验教师：苏婷



2020年11月24日星期二

# 实验课程安排与考核标准

**实验课程共16个学时，7个实验项目，总成绩为30分（30%）。**

**实验项目**

| 项目编号 | 实验一 | 实验二 | 实验三 | 实验四 | 实验五 | 实验6 |
|---|---|---|---|---|---|---|
| 学时数 | 4 | 2 | 2 | 4 | 2 | 2 |
| 实验项目 | 古典密码算法实验 DES密码算法实验 | AES密码算法实验 | 分组模式 | RSA加密算法实验 | SHA-1/MD5算法实验 | 数字签名算法实验 |
| 分数数 | 6 | 4 | 3 | 5 | 4 | 5 |

**考核方式**

- 源代码和结果截图：每次课程均需提交实验程序源代码，以及程序的运行结果截图。
- 实验报告(3分)：最后一次课程需提交实验报告，参照提供的报告模板，于实验课结束一周内提交电子版实验报告。
- 附加题累加到总分中计算，1-2分不等。

**禁止抄袭，发现雷同，本次实验双方都是0分。**


# 实验目的

- 了解AES的5种工作模式
- 掌握CBC和CTR的具体实现
- 编程分别实现 CBC 和 CTR 模式下的 AES 加密解密。


# 实验内容

1、 给出2份明文、密钥（128位）和初始IV（128位），分别用CBC 模式和用CTR 模式AES加密，实现其中一种模式进行加密。

2、CBC模式下采用PKCS7Padding填充方式；

3、相关内容放在aes_test.txt的文件中，可通过读取文件，也可从终端输入输出。

4、扩展（选做）：实现两种加密模式或者CTR模式下计数器的随机生成。

# 实验原理—分组模式

| 模式 | 名称 | 优点 | 缺点 | 备注 |
| --- | --- | --- | --- | --- |
| ECB模式 | Electronic CodeBook 电子密码本模式 | • 简单<br>• 快速<br>• 支持并行计算（加密、解密） | • 明文中的重复排列会反映在密文中<br>• 通过删除、替换密文分组可以对明文进行操作<br>• 对包含某些比特错误的密文进行解密时，对应的分组会出错<br>• 不能抵御重放攻击 | 不应使用 |
| CBC模式 | Cipher Block Chaining 密文分组链接模式 | • 明文的重复排列不会反映在密文中<br>• 支持并行计算（仅解密）<br>• 能够解密任意密文分组 | • 对包含某些错误比特的密文进行解密时，第一个分组的全部比特以及后一个分组的相应比特会出错<br>• 加密不支持并行计算 | 推荐使用 |
| CFB模式 | Cipher-FeedBack 密文反馈模式 | • 不需要填充（padding）<br>• 支持并行计算（仅解密）<br>• 能够解密任意密文分组 | • 加密不支持并行计算<br>• 对包含某些错误比特的密文进行解密时，第一个分组的全部比特以及后一个分组的相应比特会出错<br>• 不能抵御重放攻击 | • 现在已不使用<br>• 推荐用 CTR 模式代替 |
| OFB模式 | Output-FeedBack 输出反馈模式 | • 不需要填充（padding）<br>• 可事先进行加密、解密的准备<br>• 加密、解密使用相同结构<br>• 对包含某些错误比特的密文进行解密时，只有明文中相对应的比特会出错 | • 不支持并行计算<br>• 主动攻击者反转密文分组中的某些比特时，明文分组中相对应的比特也会被反转 | 推荐用 CTR 模式代替 |
| CTR模式 | CounTeR 计数器模式 | • 不需要填充（padding）<br>• 可事先进行加密、解密的准备<br>• 加密、解密使用相同结构<br>• 对包含某些错误比特的密文进行解密时，只有明文中相对应的比特会出错<br>• 支持并行计算（加密、解密） | 主动攻击者反转密文分组中的某些比特时，明文分组中相对应的比特也会被反转 | 推荐使用 |

图片来自《图解密码技术》

# 实验原理—填充方式

- ZeroPadding，数据长度不对齐时使用0填充，否则不填充。
- PKCS7Padding，假设数据长度需要填充n(n>0)个字节才对齐，那么填充n个字节，每个字节都是n;如果数据本身就已经对齐了，则填充一块长度为块大小的数据，每个字节都是块大小。
- PKCS5Padding，PKCS7Padding的子集，块大小固定为8字节。
- ISO 10126 Padding，最后一个字节是填充的字节数（包括最后一字节），其他全部填随机数。
- ANSI X9.23最后一个字节是填充的字节数（包括最后一字节），其他全部填0。

# 实验原理-PKCS7Padding

- PKCS7 填充字符串由一个字节序列组成，每个字节填充该字节序列的长度。

  pad = BlockSize – len%BlockSize;

  填充字节长度(内容): pad , len: 待加密明文字符长度，BlockSize: 分块大小

- 假定块长度为16，以三种不同长度的明文(16进制)加以说明
  - ✓ 明文长度小于16

    明文：00 01 02 03 04 05 06 07 08 09

    填充后： 00 01 02 03 04 05 06 07 08 09 06 06 06 06 06 06
  - ✓ 明文长度等于16

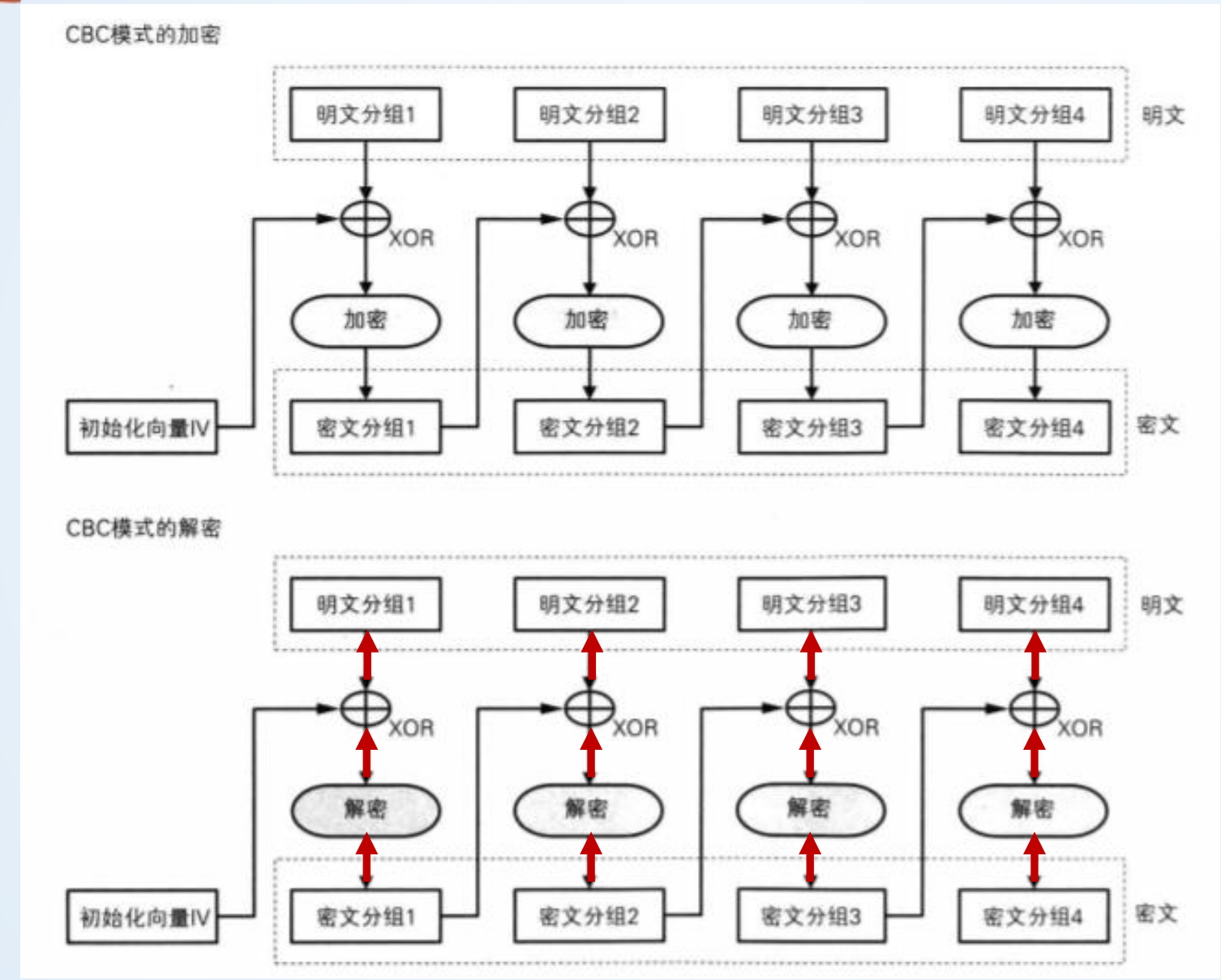
    明文： 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

    填充后： 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10
  - ✓ 明文长度大于16

    明文： 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00 01 02

    填充后： 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00 01 02 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D

# 实验原理-CBC模式




- 分块
- 对$Ci-1\oplus$明文i 加密
- 对最后一个分组填充加密

注意：如果明文长度是分块的整数倍，也要增加一个分组进行填充，否则不能解密。

# 实验原理-CBC模式

- CBC模式先将明文分组与上一次的密文块进行按比特异或，然后再进行加密处理。
- 这种模式必须选择一个初始向量c0=IV，用于加密第一块明文。
- 加密过程为

$$c_i = E_k(p_i \oplus c_{i-1})$$

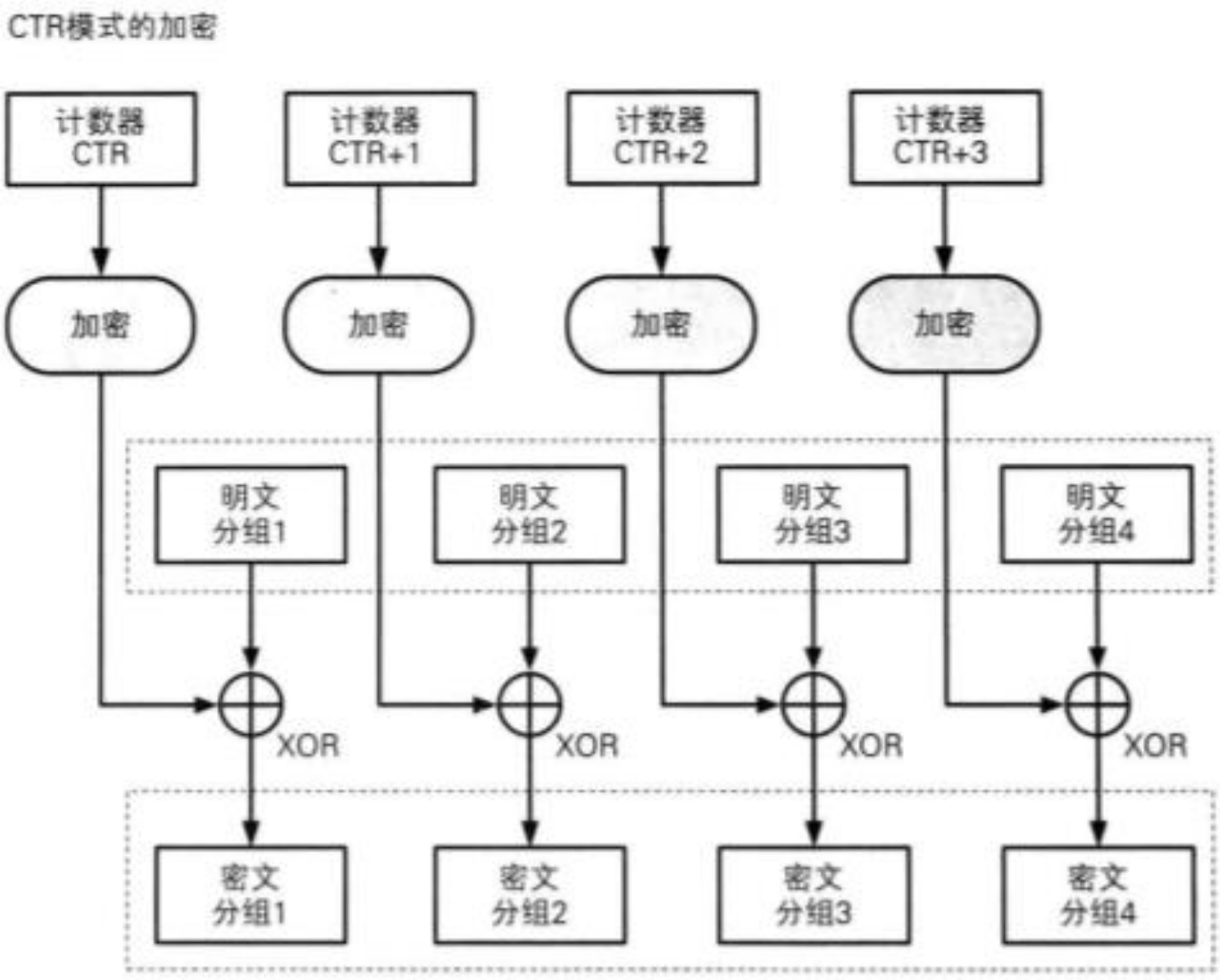
- 解密过程为

$$p_i = D_k(c_i) \oplus c_{i-1}$$

$IV_i$ --- 累加的计数器
$p_i$ --- 明文
$c_i$ --- 密文
$E_k$ --- 加密算法
$D_k$ --- 解密算法

Tips：解密最后一个分组时，需要根据解密后最后一个字节的值，删除对应填充的内容。

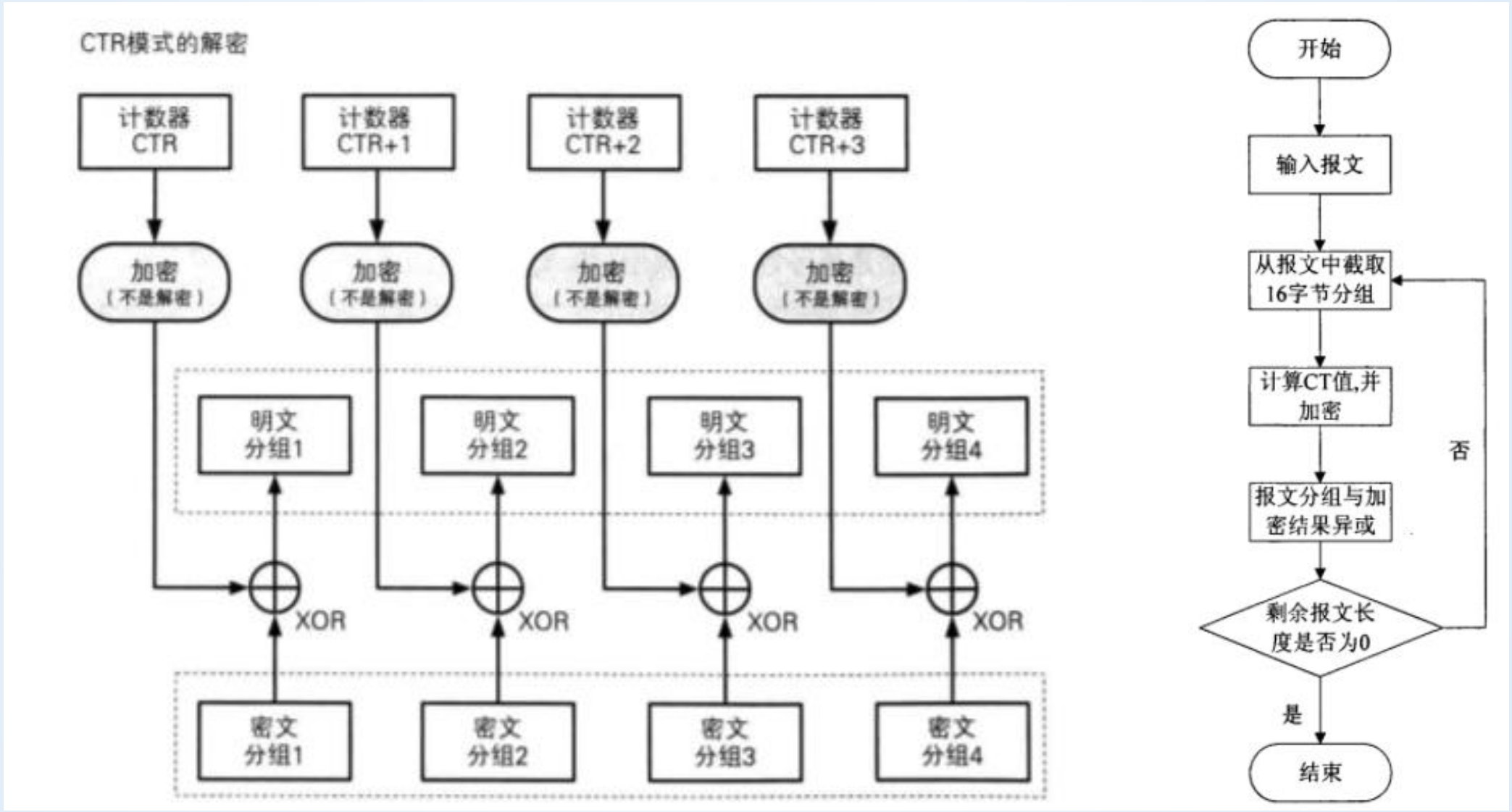
# 实验原理-CTR




计数器增加时，注意从最后一个字节增加；

如果最后一个字节已经增加到11111111，则倒数第二个字节开始增1，依次类推。

# 实验原理-CTR


CTR模式的解密
计数器 CTR
计数器 CTR+1
计数器 CTR+2
计数器 CTR+3
加密 （不是解密）
加密 （不是解密）
加密 （不是解密）
加密 （不是解密）
明文 分组1
明文 分组2
明文 分组3
明文 分组4
XOR
XOR
XOR
XOR
密文 分组1
密文 分组2
密文 分组3
密文 分组4
开始
输入报文
从报文中截取 16字节分组
计算CT值,并 加密
报文分组与加 密结果异或
剩余报文长 度是否为0
否
是
结束

# 实验原理

- **CTR**模式是一种通过将逐次累加的计数器进行加密来生成密钥流的流密码。
- 最终的密文分组是通过将计数器加密得到的比特序列（密钥流），与明文分组进行XOR得到。
- 加密过程为

$$c_i = E_k(IV_i) \oplus p_i$$

- 解密过程为

$$c_i = E_k(IV_i) \oplus c_i$$

$IV_i$ --- 累加的计数器
$p_i$ --- 明文
$c_i$ --- 密文
$E_k$ --- 加密算法


# 实验内容

1、 给出2份明文、密钥（128位）和初始IV（128位），分别用CBC 模式和用CTR 模式AES加密，实现其中一种模式进行加密。

2、CBC模式下采用PKCS7Padding填充方式；

3、相关内容放在aes_test.txt的文件中，可通过读取文件，也可从终端输入输出。

4、扩展（选做）：实现两种加密模式或者CTR模式下计数器的随机生成。

# 实验要求

## ➢ 截止时间

① 两周时间内提交（**2020-12-8 00:00**）

② 平台链接 http://10.249.182.83:8000/#/login

用户名/密码：学号/学号

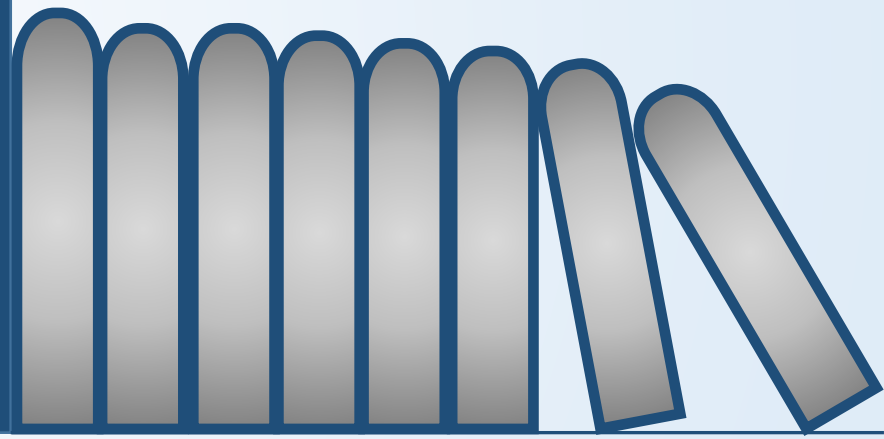
初次登录，请修改密码！

## ➢ 提交内容

① 将源码和截图文件打车zip包上传

② 以学号_姓名命名

# 谢谢




# 实验原理-CTR

计数器的每一个分组大小均为128bit，是由32为的Nonce值（一次性随机数）、64bit的IV值以及32bit的分组计数器构成。

扩展部分，本次实验我们简化计数器，根据给定的值完成，不需要随机生成。