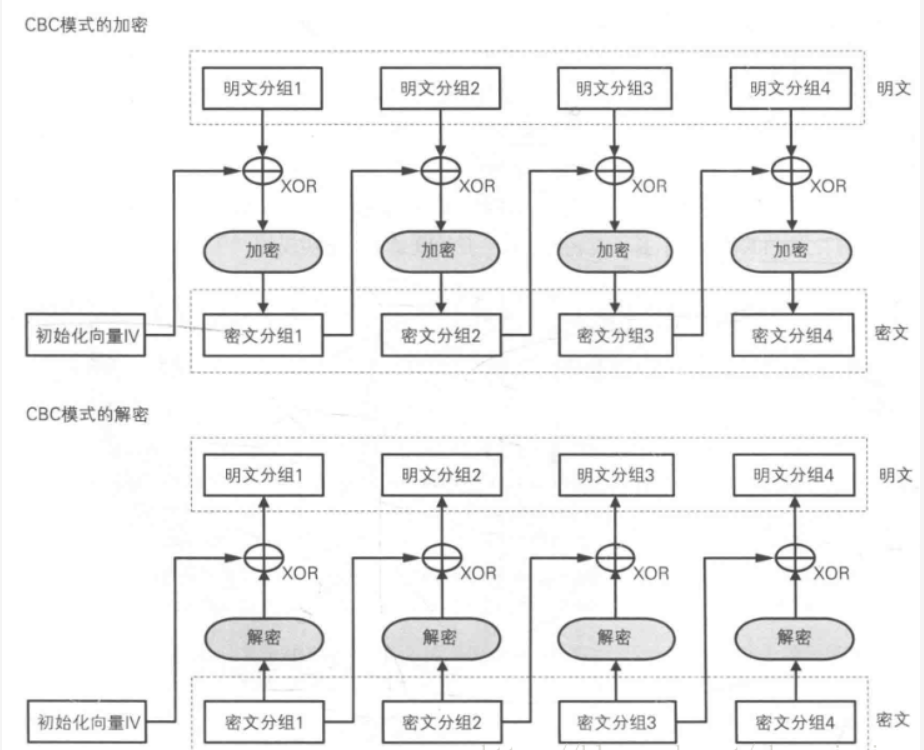
[（转）CBC模式和ECB模式解读 - wangle100 - 博客园 (cnblogs.com)](https://www.cnblogs.com/wangle1001986/p/11468419.html)

ECB（电子密本方式）其实非常简单，就是将数据按照8个字节一段进行DES加密或解密得到一段段的8个字节的密文或者明文，最后一段不足8个字节（一般补0或者F），按照需求补足8个字节进行计算（并行计算），之后按照顺序将计算所得的数据连在一起即可，各段数据之间互不影响。有利于并行计算；误差不会被传递；

CBC模式的全称是Cipher Block Chaining模式（密文分组链接模式）。在CBC模式中，首先将明文分组与前一个密文分组进行XOR运算，然后再进行加密。



假设CBC模式加密的密文分组中有一个分组损坏了。在这种情况下，只要密文分组的长度没有发生变化，则解密时最多只有2个分组受到数据损坏的影响。假设CBC模式的密文分组中有一些比特缺失了，那么此时即便只缺失1比特，也会导致密文分组的长度发生变化，此后的分组发生错位，这样一来，缺失比特的位置之后的密文分组也就全部无法解密。

为什么私钥会比公钥长

RSA体制下私钥和公钥是可以互换的。但人们之所以习惯把长的作为私钥，短的作为公钥，是为了方便公钥的分发过程，也可以缩短加密用的时间。