图解密码技术：分组密码加密模式

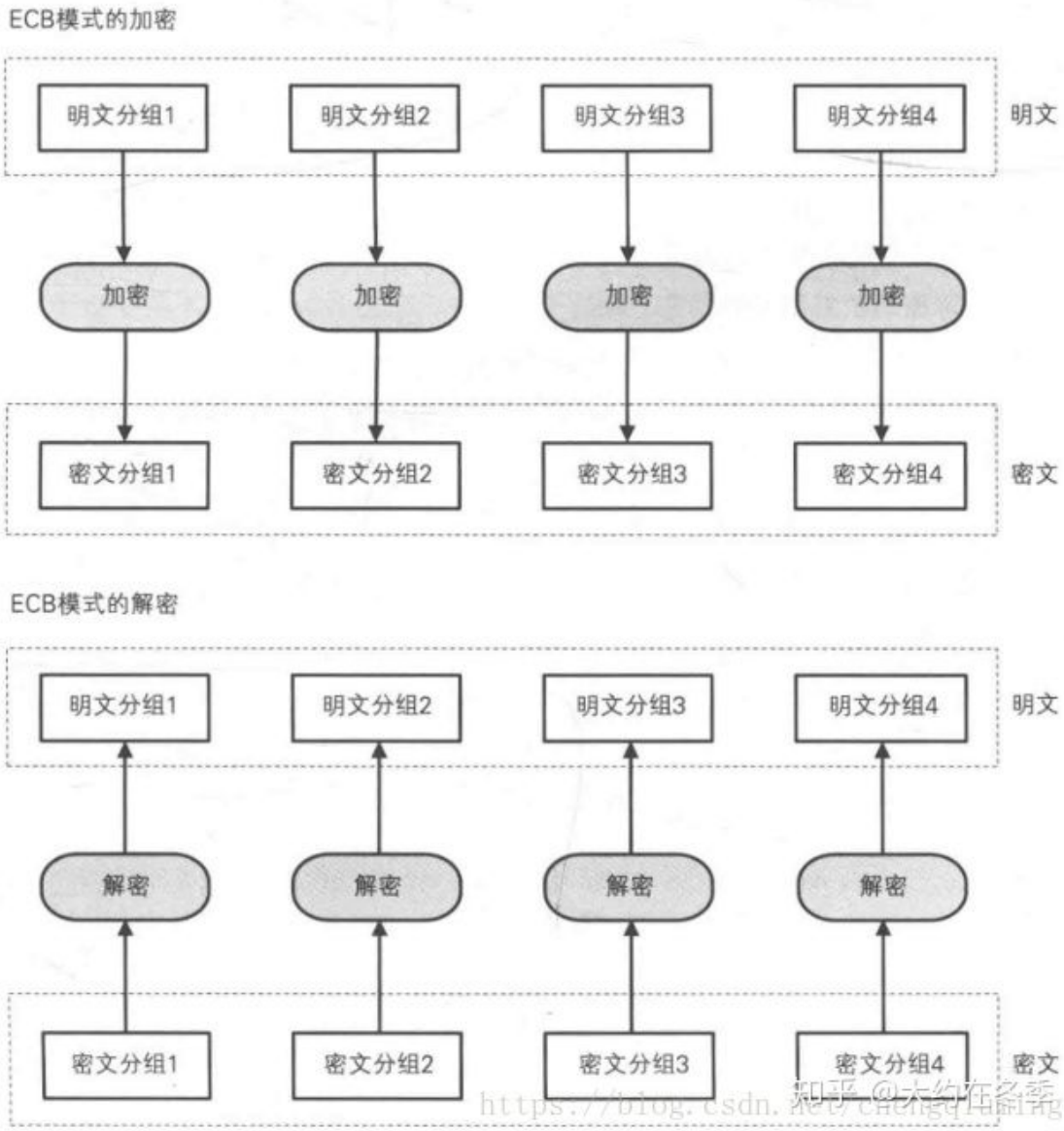
大约在冬季
信息安全

在分组密码中，一般所选用的密码算法都是公开的，加密过程中，只有密钥是保密的。一旦密钥固定，那么可以将加解密过程视为一个映射，例如AES算法，每加密一次，就可以视为128bit到128bit的数据映射。

在实际加密中，一般加密的数据不会只有几百bit，而是几mb，甚至几gb。这样，加密过程就是每加密128bit接着再加密128bit，直至将全部数据加密完。那么，就有几种常见的加密模式。

一. ECB模式

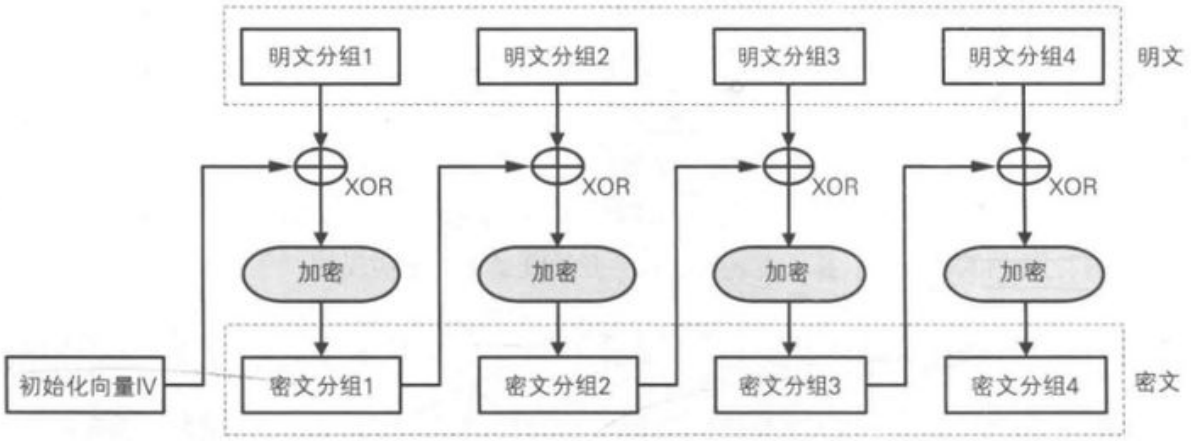
这是最简单最普通的加密模式，就是加密完一轮数据，接着加密下一轮数据，不同轮次之间的数据间无任何关系，如下图所示：



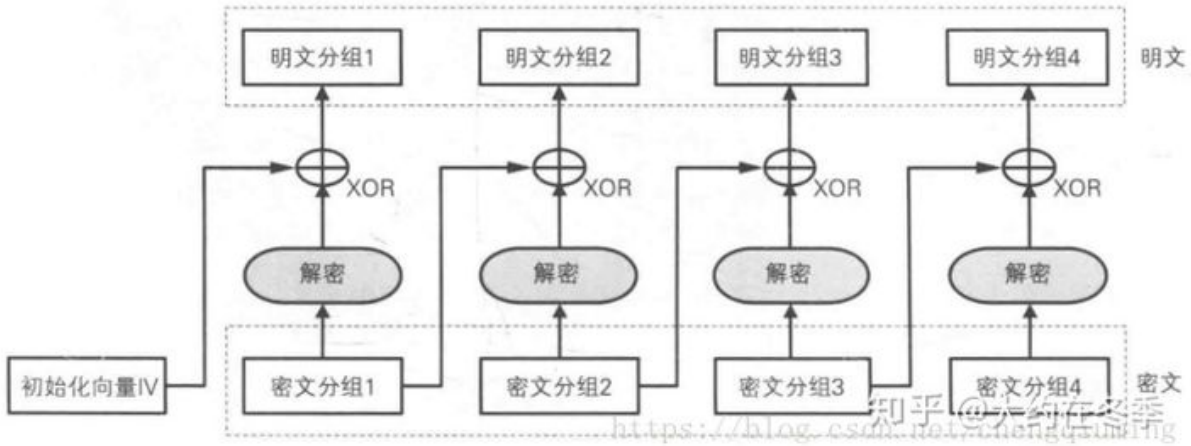
二. CBC模式

这种模式就是上面一轮加密的结果与下一轮的明文进行异或，然后进行加密。因为第一个明文分组没有前面的密文与之异或，故需要一个初始向量IV。

CBC模式的加密

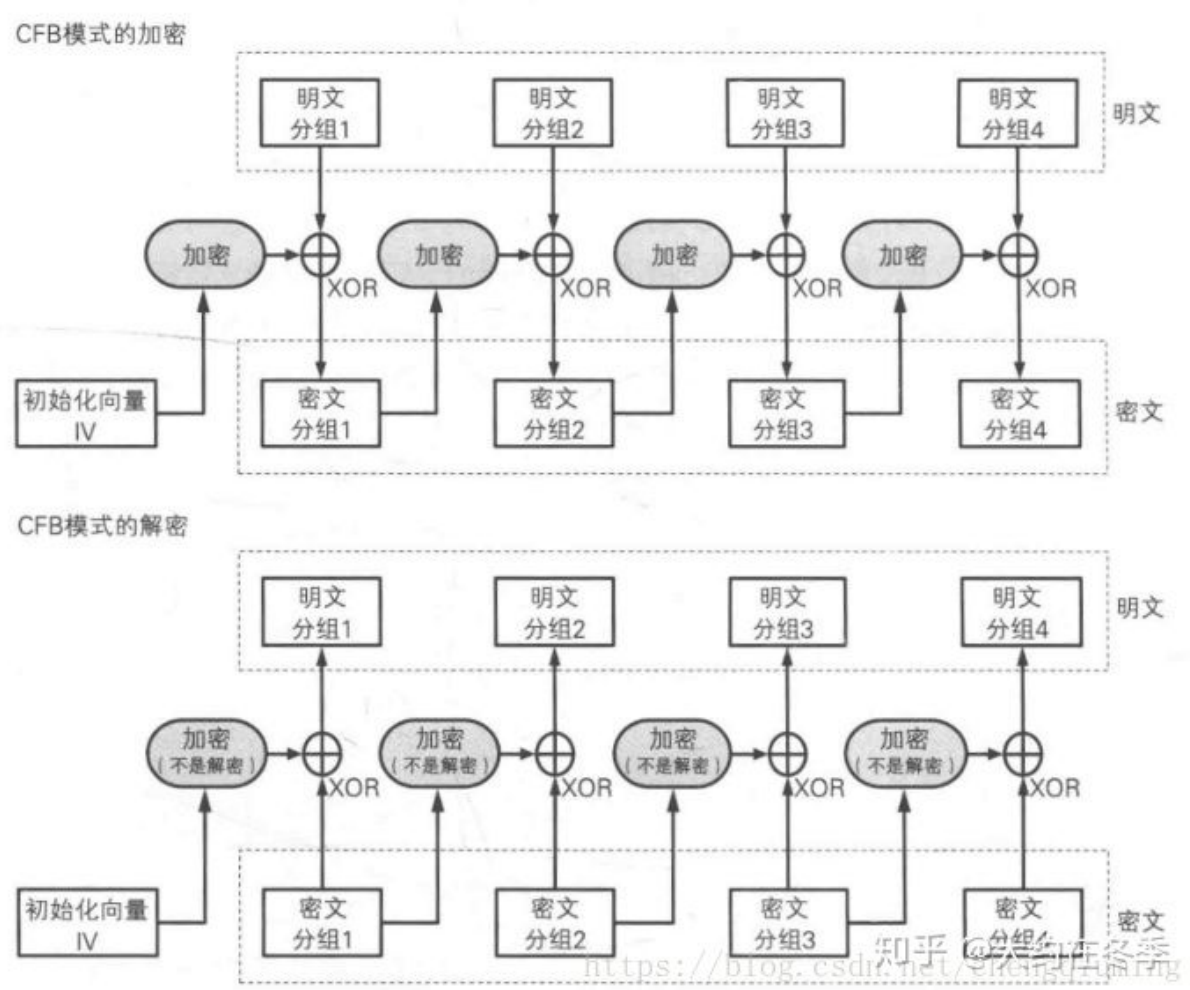


CBC模式的解密



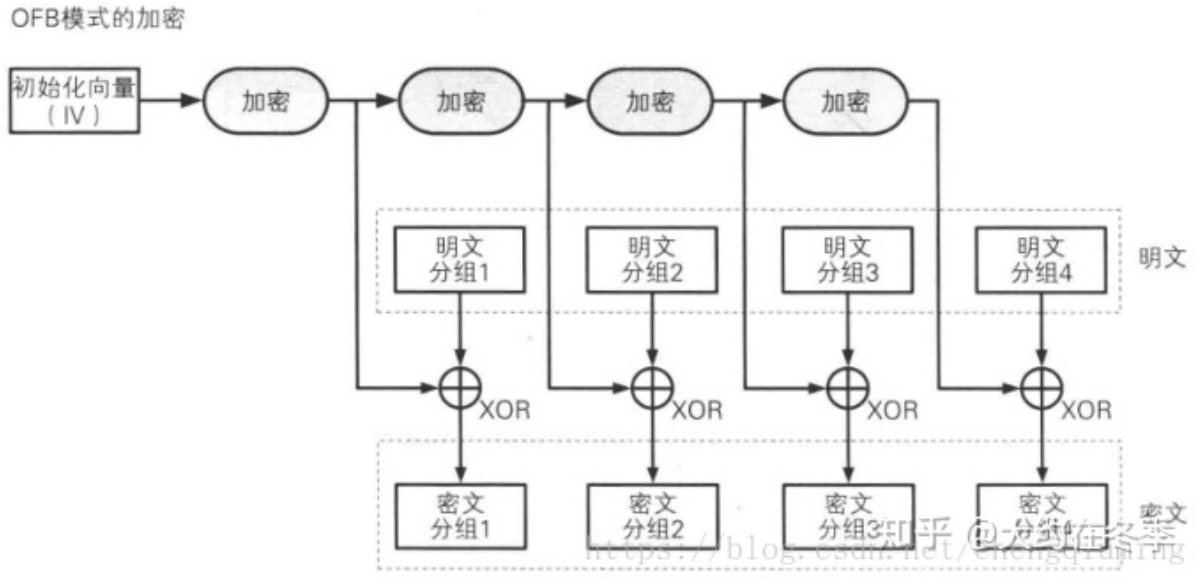
三. CFB模式

将数据进行加密的结果与明文进行异或得到密文，然后再将密文进行加密再与明文异或得到下一个密文，依次类推。同理，在最开始的时候需要一个初始向量IV。

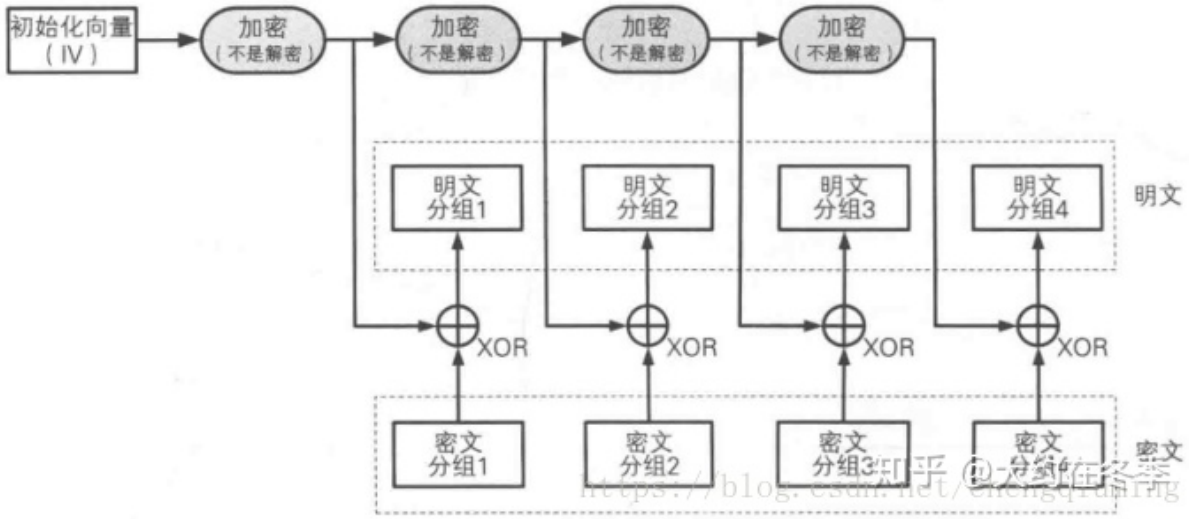


四. OFB模式

将一个初始向量一直加密，每加密一次的结果与明文进行异或得到密文。



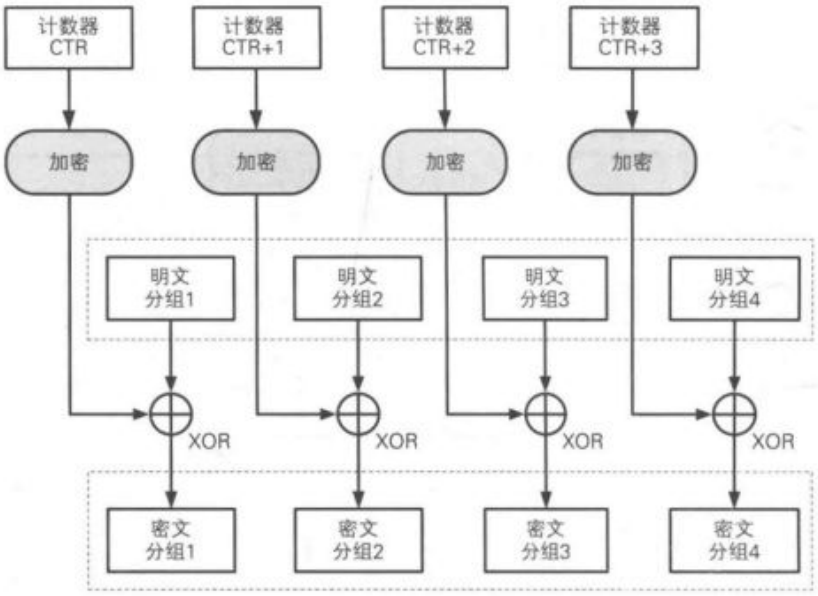
OFB模式的解密



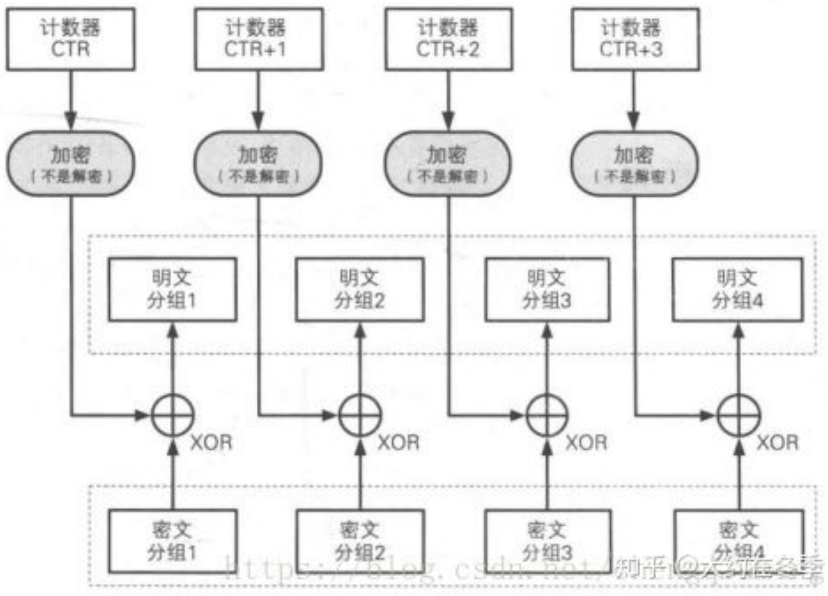
五. CTR模式

一直加密计数器，得到加密的结果与明文进行异或得到密文。

CTR模式的加密



CTR模式的解密



模式	名称	优点	缺点
ECB 模式	Electronic CodeBook 电子密码本模式	• 简单 • 快速 • 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 • 通过删除、替换密文分组可以对明文 • 对包含某些比特错误的密文进行解 的分组会出错 • 不能抵御重放攻击
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 • 支持并行计算（仅解密） • 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 个分组的全部比特以及后一个分组的 出错 • 加密不支持并行计算
CFB 模式	Cipher-FeedBack 密文反馈模式	• 不需要填充（padding） • 支持并行计算（仅解密） • 能够解密任意密文分组	• 加密不支持并行计算 • 对包含某些错误比特的密文进行解密 分组的全部比特以及后一个分组的相应 • 不能抵御重放攻击

模式	名称	优点	缺点	备注
OFB 模式	Output-FeedBack 输出反馈模式	• 不需要填充（padding） • 可事先进行加密、解密的准备 • 加密、解密使用相同结构 • 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 • 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） • 可事先进行加密、解密的准备 • 加密、解密使用相同结构 • 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 • 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