蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

对称加密算法下

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

- 了解四种对称加密模式：ECB、CBC、CFB、OFB

01 对称加密模式简介

对称加密模式简介

对称加密模式简介

什么是分组加密

- 对明文加密方式的不同，密码体制分为：流加密和分组加密。
- 流加密是针对明文每一个比特或者字母进行加密，分组加密是把明文切割成固定大小然后进行加密。

分组加密模式

- 明文的长度不固定，而分组密码只能处理特定长度的一块数据，这就需要对分组密码的算法进行迭代，以便将一段很长的明文全部加密，而迭代的方法就是分组的模式。

02 ECB、CBC、CFB、OFB

ECB - Electronic Code Book, 电子密码本模式

CBC - Cipher Block Chaining, 密码块链模式

CFB - Cipher FeedBack, 密文反馈模式

OFB - Output-Feedback, 输出反馈模式

ECB - Electronic Code Book, 电子密码本模式

ECB

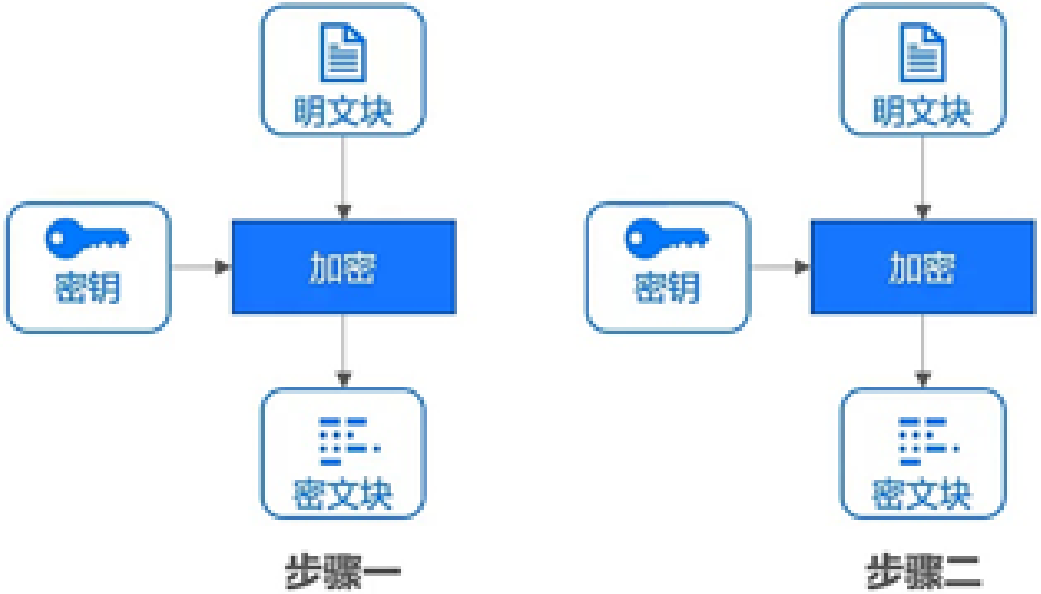
- 数据分成固定大小的数据块，然后对每个数据块使用密钥进行加密得到密文，最后将所有的密文连在一起得到最终密文。

优点:

1. 简单;
2. 有利于并行计算;
3. 不存在误差传递。

缺点:

1. 不能隐藏明文的模式;
2. 可能对明文进行主动攻击。



CBC - Cipher Block Chaining, 密码块链模式

CBC

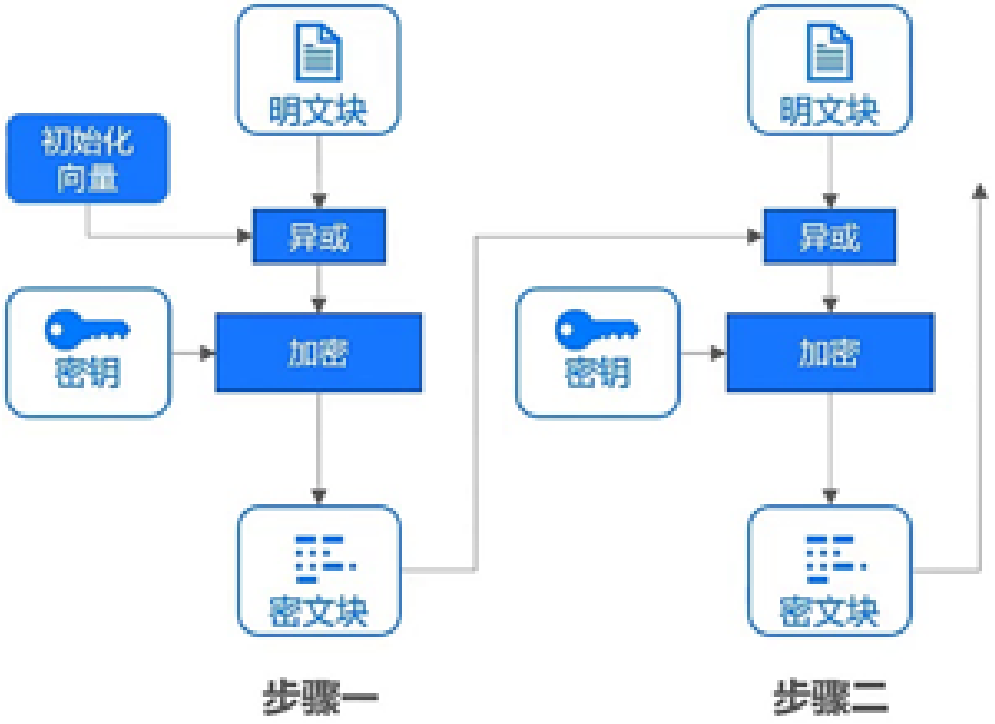
- 一个明文块在被加密之前要与前一个的密文块进行异或运算。还需协商一个初始化向量，这个初始化向量没有实际意义，只是在第一次计算的时候需要用到而已。

优点:

不容易主动攻击,安全性好于ECB,适合传输长度长的报文,是SSL、IPSec的标准。

缺点:

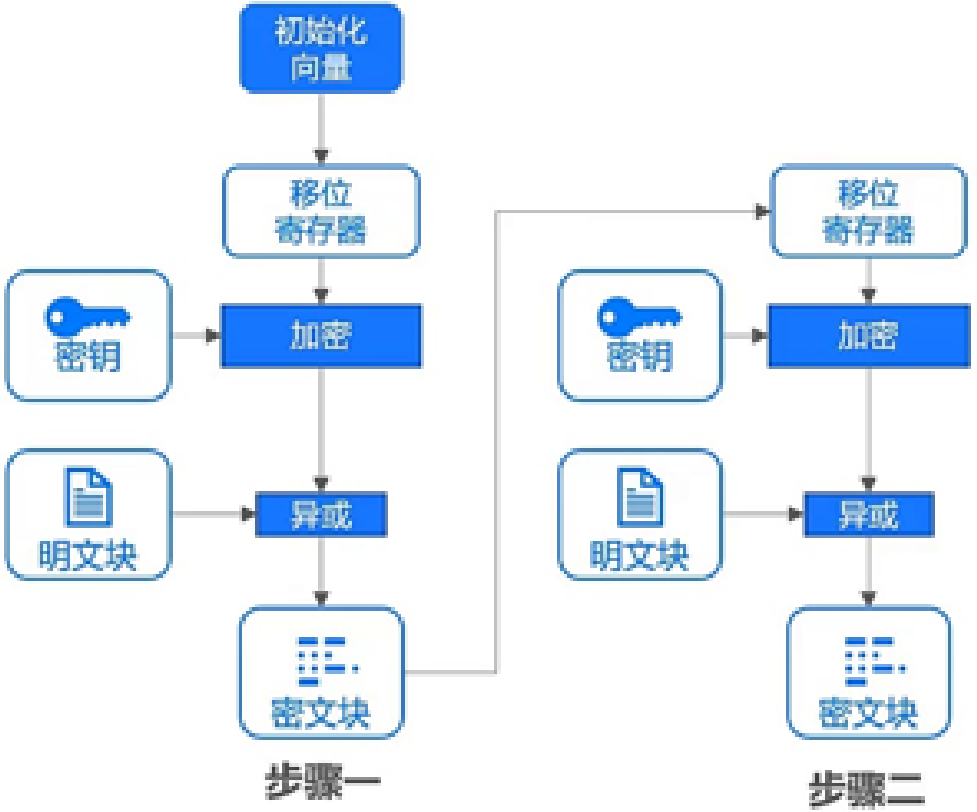
1. 不利于并行计算
2. 误差传递
3. 需要初始化向量



CFB - Cipher FeedBack, 密文反馈模式

CFB

- 需要使用一个与块的大小相同的移位寄存器，并用初始化向量将寄存器初始化。
- 接下来将寄存器内容使用块密码加密；
- 然后将结果与明文块进行异或，以产生密文块。
- 下一步将生成的密文块移入寄存器中，并对下面的明文块重复这一过程。



优点：

1. 隐藏了明文模式；
2. 分组密码转化为流模式；
3. 可以及时加密传送小于分组的数据；

缺点：

1. 不利于并行计算
2. 误差传递
3. 唯一的IV

OFB - Output-Feedback, 输出反馈模式

OFB

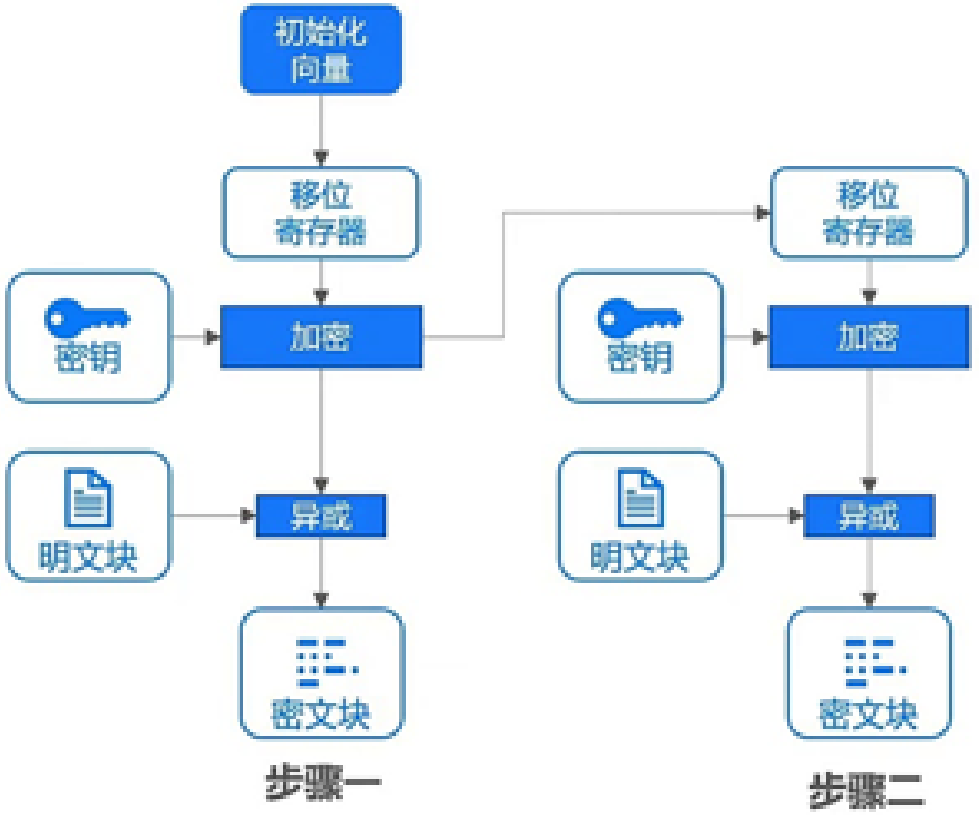
- 和CFB唯一的区别是，参与下一次加密使用的是移位寄存器与密钥加密之后的结果，而不是密文块。

优点:

1. 隐藏了明文模式;
2. 分组密码转化为流模式;
3. 可以及时加密传送小于分组的数据。

缺点:

1. 不利于并行计算;
2. 对明文的主动攻击是可能的;
3. 误差传递。



总结

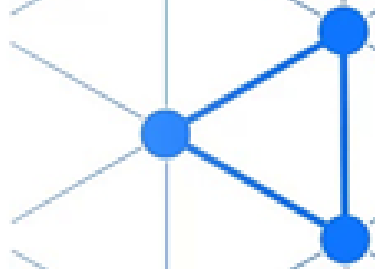
■ 对称加密简介

- 分组加密是把明文切割成固定大小然后进行加密

■ ECB、CBC、CFB、OFB

- ECB是直接对分割后的数据块进行加密
- CBC是一个明文块在被加密之前要与前一个的密文块进行异或运算
- CFB和OFB加密的区别是使用前一个密文块还是密钥流

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN