网络信息安全第三章：对称密码机制课堂笔记

多重加密

加密是一个函数，输入参数是明文，输出是密文。多重加密是对密文再输入到函数当中做一次加密。

缘起

70年代，DES提了出来。穷举和密码分析学是两种基本的攻击方式。在设计DES时，密钥只有56位。这在当时可以破除穷举攻击，但是现在不行的了。有两种思路：

1. 设计新的算法：AES——高级加密算法；但是不可能一瞬间都改成AES，更新换代成本高。
2. 改动DES：多次使用DES，使用多个密钥，增加穷举开销，计算量会非常大，以达到安全的要求。

双重DES

> 进行两次加密。密钥长度112位。

$$C = E_{K2}(E_{K1}(P))$$
$$P = D_{K1}(D_{K2}(C))$$

这就好像将第一次加密的密文再次进行加密。就像快餐汉堡的面包会把现成的面包的底面煎一下一样。

为什么不用双重DES，用三重DES呢?

中途相遇攻击!

中途相遇攻击

$$X = E_{K1}(P) = D_{K2}(C)$$

尝试对k1作加密操作，对k2做解密操作。使用两次穷举攻击可以得到一组加解密结果，它们具有相同的中间值x。这时，我们就可以彻彻底底的知道加密密钥k1和解密密钥k2的值了。

它的细节是这样的：

1. 首先对明文按所有可能的密钥进行加密，将结果值按照一定顺序放到一张表里。这就好像把所有面包店的面包胚都买下了。
2. 将密文用所有可能的密钥进行解密，每解密一次就将结果和表中对应行的值进行比较，如果相等就立刻用这个密钥去破译新的密文，如果得到了正确的明文，就说明这是我们想要的密钥。这就好像根据煎好的面包比对原始的面包胚。

注意：这种攻击对两次加密的分组密码都是好用的!

三重DES

> 两个密钥，三次加密

$$C=E_{K1}[D_{K2}[E_{K1}[P]]]$$

第二步采用解密算法并没有什么密码学上的深刻含义，仅是为了使用三重DES的用户可以利用该算法解密单DES的数据。

其实，使用三重DES也可以使用”三个密钥，三次加密“，即将最外侧的K1换为K3，只要K1 = K2 或 K2 = K3就可以兼容，有些基于Internet的应用已经采用了这种方法。

工作模式

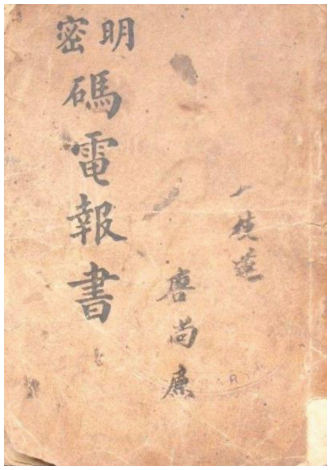
DES只是分组算法，怎么使用是另外一回事。对称密码在实际应用中有5种实际的使用模式，这非常重要。本节主要介绍这些对称式算法是怎么执行的，和对应的优缺点。这些模式就正如之前所说的没有优劣之分，不同的模式会适用于不同的场景。

> 定义：工作模式是一项增强密码算法或使算法适用具体应用的技术。

电子密码本（ECB）

明文分成64的分组进行加密，如果不够时需要填充。每个分组用同一密钥加密，相同明文分组加密得相同密文。这就好像我们面前摆放着一大本密码本，每次我们的拿了一个64位的明文，只需要将它翻阅密码本就能翻到和它等长的64位密文。

> 描述：用相同的密钥分别对明文分组独立加密。



缺点

1. 明文分组和密文分组等长
2. 消息很长且结构化（如关系型数据库的关系表，某些信息会重复出现：如性别、职称、部门），利用密码分析学可以根据结构判断明文内容。

优点

特别适合与数据较少的情况，比如加密密钥。想要安全传输一个DES或AES密钥，这种方式是非常合适的。

密文分组链接模式（CBC)

> 加密输入是当前密文分组和前一密文分组的异或，形成一条链。使用相同的密钥，这样每个明文分组的加密函数输入与明文分组之间不再有固定的关系。若有重复的明文分组，加密后便看不出来。

初始向量IV必须为收发双方共享，且第三方不能预测，IV不能不经授权就进行修改，可以使用ECB对IV进行加密后再发送。否则攻击者可以欺骗接收者，将明文的第一个分组的某些位取反。

计算IV

1. 随机数生成
2. 加密时变值

优点

1. 密文分组依赖于其他明文分组

密码反馈模式（CFB）

> 将DES转换成流密码。不再要求报文填充成整个分组，可以实时运行，每个字符可以使用流密码技术传输。

缺点

1. 比特差错传播：由于噪声造成的比特差错会导致后续的加密过程继承。

输出反馈模式（OFB）

> 结构上与密码反馈模式类似，它使用加密函数的输出填充移位寄存器而不是使用密文单元填充移位寄存器。这样后续的解密不会受比特差错的干扰。

缺点

1. 抗消息流篡改攻击的能力不如CFB。攻击者可以篡改密文的某些比特，恢复出的明文相应位也取反，接收方可能无法识别。CFB中如果密文改变的话，会发现后面的明文全部乱了，接收端就能发现问题，让发送方进行重传了。
2. 不能实现并行。

优点

比特差错不会扩散。

计数器模式（CTR）

> 加密的是计数器的值而不是反馈值

优点

1. 适用于高速网络，因为可以实现并行。方法是可以并行的。不必等到前一个分组算完后再进行下一分组的加密。

注意

密钥和计数器的值不可重复使用。