# 加密学基础（密码实现技术）

<https://blog.csdn.net/folian1989/article/details/79920766>

一、密钥管理概念

  1、密钥生成

        安全的生成密钥：即生成可信任的密钥，保证用户得到的密钥是安全的，生成密钥的机器或程序是可信的 。

        生产安全的密钥：一般来说是指密钥抗猜测和抗穷举等针对密钥攻击的能力。涉及密钥长度和密钥强弱的问题。

 2、密钥分发

        通信双方要进行安全的通信，首先需要协商密钥，尤其对于对称加密算法，双方必须先取得同样的加密密钥 （会话密钥），公开密钥算法更好地解决了这个问题 。

3、密钥验证

        密钥验证包括两方面的内容：一是验证密钥的发送方是可信的；二是验证密钥确实是正确和完整的 。

        较好的办法是利用单向散列函数， 因为单向散列函数对数据的微小变化十分敏感。

4、密钥的使用

        一种是使用软件进行加密，一种是使用硬件进行加密。软件加密是较常使用而不安全的方式。利用硬件进行加密是一个更安全的方案 。

5、密钥的存储

        密钥存储最常用的方式或许是存储在人的大脑中 ，更安全的方式是存储在硬件中或者存储器中。如存储在智能卡 中。

6、密钥销毁

        一般来说，密钥都有一定的使用寿命，因为密钥使用的时间越长，其泄漏和受攻击的危险就越大。 到了有效期之后，更换新的密钥，同 时 销 毁 旧 的 密钥。销毁旧密钥很重要，可以避免攻击者用旧密钥解密以前他截取到的信息。

7、公钥管理

       只要保证该公钥是可信任的即可。较好的方法是通过可信任第三方的数字签名来确认这个问题，目前比较系统化和标准的应用方法就是数字证书。 通常签发数字证书的可信任第三方机构称为证书验证中心 （ＣＡ）

二、加密算法

1、概述

        通常密码算法的加密模式应该考虑：算法加密模式的安全性 、容错性 、效率 、实时性 。

        加密算法又分为对称加密、非对称加密、摘要算法；

2、对称加密算法

1）分组加密

        分组加密又称为块加密，是将要处理的数据分成固定的长度，然后在这固定长度的数据上使用密码算法进行计算。

A、电子密码本模式 （ＥＣＢ）

        最简单的分组加密模式，也是最能体现 “分组”概念的加密模式。它将加密的数据分成若干组，每组的大小跟加密密钥长度相同，然后每组都用相同的密钥进行加密。

        电子密码本模式有以下特点：

        \* 每次加密的数据长度固定。

        \*各个分组相互独立，可以并行加密和解密。

        \*相同的明文使用相同的密钥总是产生相同的密文。

        \*一个位的错误只对所在的明文块产生影响，但是增加或删除一个位会导致其后整个密文序列没有办法正确解密

B、加密分组链接模式 （ＣＢＣ）

       可以解决电子密码本模式容易受到分组替换攻击的问题 。

         加密分组链接模式首先也是将明文分成固定长度 的 分 组， 然 后 将 前 面 一 个 加 密 分 组 输 出的密文与下一个要加密 的明 文分组 进行 异 或 操 作 计 算， 将计算结果再用密钥进行加密得到密文。第一明文分组加密的时候， 因 为 前 面 没 有 加密 的 密 文， 所以 需 要 一 个 初 始化向量 （ＩＶ）。

加密分组链接具有以下的一些特点：

        \*每次加密的数据长度固定。

        \*当相同的明文使用相同的密钥和初始向量的时候 ＣＢＣ 模式总是产生相同的密文。

        \*链接操作使得密文分组要依赖当前和以前处理过的明文分组，密文分组顺序不能列进行重新排列，也不能进行并行操作。

        \*可以使用不同的初始化向量来避免相同的明文产生相同的密文，能一定程度上抵抗字典攻击等密文分析

        \*一位发生错误后，会对当前及后一个分组的明文产生错误。增加或删除一个位会导致其后整个密文序列没有办法正确解密

        \*不能实时解密，必须等到８个字节都接收到之后才能开始解密，否则得不到正确的结果

C、加密反馈模式 （ＣＦＢ）

        加密反馈模式通过引入移位寄存器来克服加密分组链接模式不能实时解密的困难。

加密反馈模式具有以下特点：

每次加密的数据不超过６４位。

当使用相同的密钥和初始向量的时候，相同明文使用 ＣＦＢ 模式加密输出相同的密文。

链接操作的方法使得密文数据依赖当前和以前所有的数据，所以数据都应该按顺序组织在一起，不能进行并行计算操作。

可以使用不同的初始变量使相同的明文产生不同的密文，防止字典攻击等密文分析行为。

ＣＦＢ模式的强度依赖于密钥的长度，强度最大的情况是每次加密的数据长度和密钥长度相同的情况。

当每次加密的数据长度的取值比较小的时候，相同的明文一般需要更多的循环来完成加密，这可能会导致过大的开销。

每次加密数据的位数应该为８的整数倍。

一旦某位数据出错，会影响到目前和其后一些字节的加密数据的正确解密，但是对同步错误具有自恢复功能。

数据可以实时传输，每接收到一位都可以随即进行解密。

D、输出反馈模式 （ＯＦＢ）

        跟加密反馈模式相似，只是输入寄存器的数据不一样。输入寄存器的数据从加密算法输出的分组的前８位数据取得 （对于加密数据长度为８位的输出反馈模式）。

        输出反馈模式的特点如下：

每次加密的数据不超过６４位。

当使用相同的密钥和初始向量的时候，相同明文使用 ＯＦＢ模式加密输出相同的密文。要注意的是，在 ＯＦＢ模式下相同的密钥和初始向量产生相同的密钥流，所以，为了安全原因，一个特定的初始向量对一个给定的密钥应该只使用一次。

因为没有使用链操作，数据相关性小，所以使得 ＯＦＢ模式更容易受到攻击。

可以使用不同的初始变量产生不同的密钥流，从而使得相同的明文使用相同密钥产生不同的密文。

当每次加密的数据长度取值比较小的时候，相同的明文一般需要更多的循环来完成加密，这可能会导致过大的开销。

每次加密数据的位数应该为８的整数倍。

ＯＦＢ模式不会进行错误传播，某位密文发生错误，只会影响该位对应的明文，而不会影响别的位。

ＯＦＢ模式不是自同步的，如果加密和解密两个操作失去同步，那么系统需要重新初始化。

每次重新同步的时候，应该使用不同的初始向量。这样可以避免产生相同的密文，从而避免 “已知明文”攻击。

F、三重分组加密模式

        有两种应用方式：一种是使用两个密钥，即第一个密钥和第三个密钥相同；还有一种就是使用三个不同的密钥。

三重加密分组模式具有如下特点：

加密过程为使用 Ｋ１加密，然后使用 Ｋ２解密，最后使用 Ｋ３加密完成加密过程。

加密过程使用了电子密码本模式、加密分组链接模式等其他基本分组加密模式，但是密钥增加到了１６８ 位，虽然目前理论上可以使得有效密钥长度降到１１２ 位，相对于５６位的密钥来说，安全性还是得到了很大的提高。

如果前两个密钥是相同的，那么就相当于使用一个密钥加密了一次。

如果第一个和第三个密钥是相同的，那么密钥长度事实上是１１２位，有些攻击方法可以使得有效密钥的长度降为比５６位稍多的长度，但需要很大的内存空间。

如果三个密钥都是相同的，那么就跟普通的分组加密模式效果相同了。

三重分组加密模式的基本特点跟其使用的基本分组加密模式特点基本一致。

G、其他加密模式

计数器模式 、分组链接模式 、扩散密码分组链接模式 等；

E、数据填充

        电子密码本模式和加密分组链接模式的分组算法都要求加密输入的分组是固 定 长 度的，最后一个分组一般来说是不足一个分组长度的。通常使用填充技术对最后一个分组进行填充以使该分组正好为一个分组的固定长度。

使用规则的数据进行填充 ——密文长度跟明文长度不一样

密文挪用的分组填充——密文长度同明文长度一致

2）序列加密

序列加密模式又称为流加密方式，是对要处理的数 据 按 位（或字节）逐个进行加密处理。

A、自同步序列加密模式

        自同步序列加密模式又称为密文自动密钥，它的主要思想是密钥序列跟以前一定数量的密文位相关，即密钥序列是以前一定数量密文位的函数。

自同步序列加密模式的特点如下：

内部状态是前面ｎ 位固定长度密文的函数。

算法的安全性依赖于输出函数的复杂性和安全性。

会产生密文错误扩散，密文中一位发生错误，会导致其后ｎ 位密文不能正确解密。

解密的时候具有密钥序列和密文自动同步的功能，具有同步错误自恢复功能。

明文长度和密文长度相同。

容易受到回放攻击。

B、同步序列加密模式

        同步序列加密模式又称为密钥自动密钥加密，它的特点是密钥序列的产生跟处理的消息是不相关，相互独立的。

同步序列加密模式的特点如下：

密钥序列的产生跟明文和密文消息都无关。

不会产生密文错误扩散，但是没有同步错误自动恢复功能。

密文和明文长度相同。

3、非对称算法

        主要的RSA\DSA\DHC\ECC

RSA:1977麻省理工 目前网络上进行保密通信和数字签名的最有效的安全算法之一。其安全性基于数论中大

素数分解的困难性；目前需要采用1024位的秘钥；

DSA：不能用作加密，只用作数字签名，安全性基于解离散对数的困难性；

DH(Diffie-Hellman秘钥交换）：安全性基于有限域上计算离散对数的困难性；DH秘钥至少1024位；

ECC椭圆曲线密码体制：依据是定义在椭圆曲线点群上的离散对数问题的难解性；

        SM2 为ECC算法中一种，国家标准；

4、摘要算法

        SM3为国家标准信息摘要算法，SM2签名使用；

        单向散列函数不可逆，做数据完整性验证；MD2\MD5\SHA\SHA-1/256/383/512等

常用的MD5输出结果16字节，SHA1输出结果16字节；

5、加密算法的选择

        仅仅考虑算法实现的复杂性和数据处理速度，那么选用电子密码本模式是比较好的选择。但电子密码本模式也是最容易受到分组重复及密文分析等攻击的分组加密算法，一般不建议使用该加密模式。

        加密分组链接模式是适用于大多数文件加密的模式，它的安全性能相对不错，是加密存储文件的首选加密模式。

        需要实时解密的系统，比如需要对单个字符进行处理的系统可以选择加密反馈模式，但是该模式会产生密文错误扩散，所以在对错误扩散敏感的系统中是不能使用的。

        对容易发生密文错误的系统，可以选择输出反馈模式，因为该模式不会产生密文错误扩散，所以可以降低错误率。但是该模式安全性比较差。