**加密知识简介**

**一直对于加密相关的内容的了解很少，这里做一个简单的直观总结，便于以后查阅和学习。**

本文主要参考资料：《SSH-Unix.Secure.Shel.tool》附录A 加密技术基础

作者：QuietHeart

Email：quiet\_heart000@126.com

2011年4月29日

**什么是加密**

当还是一个小学生时，你可能经常在玩耍时使用某种方法将一张私人便条变成密码，以使除了你的伙伴以外的其他人无法了解其中的含义。当你通过其他同学传送这张便条给真正的接收人时，中间人无法读出它的含义，从而确保了安全性。这为我们引出了加密的定义。

       加密是一门通过使用一种编码而使某些可读的东西 (明文)变为不可读的东西 (密文)的科学。这些编码就是将明文变成密文的加密算法 (也称为密码)或数学方法。所以，当你和你的朋友们将信息编码时，你们正在使用简单的加密。

       有两类涉及安全信息的基本研究，它们是研究安全信息的**加密术**和研究破解安全信息密码的**密码分析学**。这两类研究都称为**密码学** 。

**传统式对称密钥加密----Caesar密码**

       例如，如果你有一个加密方法是将每个字母向右移 3个，那么，你将有一个相应的解密方法：把字母向左移 3个。如下，

       加密算法：字母＋3＝密文

       解密算法： 密文－3＝字母

       那么，例如 “l e t ’s go to the toga party!”看起来将是这样：ohw’v jr wr wkh wrjd sduwb!

       这种方法称为**Caesar密码**。有许多类似的加密方法，这样使用的加密类型，被称为**传统式对称密钥加密**，其中信息的发送者和接收者都知道编码。

**对称密钥加密和公钥加密**

**对称密钥加密**常用的算法有DES、Triple DES或IDEA加密，MD5。对称密钥加密的最大弱点就是密钥交换。

       总之，对称密钥加密通信双方持有同样的密钥对密文进行解密。

       因为对称密钥加密在密钥方面有根本上的缺陷，所以公共密钥加密在报文和网络方面的应用已成为流行。

       RSA实际上用于**公共密钥加密**，它是当前所能得到的最强的公共密钥算法。公共密钥包含两个同属于一方的密钥：一个是公共密钥，它被所有人所共享；另一个是私有密钥，归个人秘密中存。与对称密钥加密不同，公共密钥加密对加密与解密使用两把密钥。一把是秘密的，这是私有密钥，用来对密文解密。密文本身由公共密钥产生，公共密钥分发给要发送加密信息给你的人。其他人如何得到你的公共密钥？很容易，发布它即可。你—私有密钥的所有者，是惟一能对信息进行解密的人。

       尽管在保密密钥加密方面的改进，公共密钥加密仍有其弱点，它仍然需要第三方证实，仍然容易受到与对称密钥加密算法同样类型的攻击；另外，公共密钥管理(包括提出、验证、检验和废弃)引入一个全新的弱点—可能被泄露的管理结构。

       总之，每个通信方都用自己的私钥解密接收的数据，用公钥加密数据并发送给其他通信方。公钥是公共的，私钥是只有自己才有的。

**数字签名**

       数字签名常用公共密钥加密来产生签名，如 RSA和DSA。用公共密钥产生数字签名与信息加密的工作相反。

       信息通过hash函数发送。hash处理后的信息用私有密钥加密。一旦数据用私有密钥加密，任何持有公共密钥的人都能检验，它是用私有密钥产生的，这样，数据就被验证了。因此，任何持有公共密钥的人都可以进行检验。

       这里的hash函数用于产生数字签名。Hash函数(散列函数)是一个提取信息和产生一个固定长度的信息个性特征的数学函数。无论要进行hash方法的信息有多大，输出的长度都一样。

       简言之，就是将hash处理后的信息用私钥加密，其它人用公钥解密恢复成功(恢复成的应该是hash处理的结果？)表示加密的人就是你也就是数字签名的验证就成功了。