三种加密算法和两种密钥交换机制讲解

 (2012-03-06 22:35:02)

[[http://simg.sinajs.cn/blog7style/images/common/sg_trans.gif](javascript:;)转载▼](javascript:;)

|  |  |
| --- | --- |
| 标签：  [杂谈](http://search.sina.com.cn/?c=blog&q=%D4%D3%CC%B8&by=tag) |  |

**一、基础知识：**

1、互联网上中间人攻击通常用的三种方式：1）窃听 2）数据篡改 3）会话劫持

       2、数据加密的常用的三种方式有：对称加密、非对称加密、单向加密。

          3、ssl:secure socket layer,安全的套接字层。

          4、TLS：Transport Layer Security,功能类似于ssl。

          5、随机数生成器：/dev/random 和 /dev/urandom 。   -salt：依赖于随机数生成器。

          6、随机数的来源：熵池和伪随机数生成器。熵池中的随机数来自块设备中断和键盘和鼠标的敲击时间间隔；伪随机数生成器中的随机数来自于熵池和软件产生。

          7、openssl rand [base64] num 也可以用来生成随机数。

          8、echo –n “QQ”|openssl base64，表示对QQ做base64编码。

**二、对称加密：**

  1、加密方和解密方使用同一个密钥。

      2、加密解密的速度比较快，适合数据比较长时的使用。

      3、密钥传输的过程不安全，且容易被破解，密钥管理也比较麻烦。

         4、加密算法：DES（Data Encryption Standard）、3DES、AES（Advanced Encryption Standard，支持128、192、256、512位密钥的加密）、Blowfish。

         5、加密工具：openssl、gpg(pgp工具)

**三、非对称加密（公钥加密）：**

      1、每个用户拥用一对密钥加密：公钥和私钥。

      2、公钥加密，私钥解密；私钥加密，公钥解密。

      3、公钥传输的过程不安全，易被窃取和替换。

      4、由于公钥使用的密钥长度非常长，所以公钥加密速度非常慢，一般不使用其去加密。

      5、某一个用户用其私钥加密，其他用户用其公钥解密，实现数字签名的作用。

      6、公钥加密的另一个作用是实现密钥交换。

         7、加密和签名算法：RSA、ELGamal。

         8、公钥签名算法：DSA。

         9、加密工具：gpg、openssl

**四、单向加密：**

1、特征：雪崩效应、定长输出和不可逆。

     2、作用是：确保数据的完整性。

        3、加密算法：md5（标准密钥长度128位）、sha1（标准密钥长度160位）、md4、CRC-32

        4、加密工具：md5sum、sha1sum、openssl dgst。

        5、计算某个文件的hash值，例如：md5sum/shalsum  FileName,openssl dgst –md5/-sha1 FileName。

**五、密钥交换的两种机制：**

      1、公钥加密实现：发送方用接收方的公钥加密自己的密钥，接收方用自己的私钥解密得到发送方的密钥，逆过来亦然，从而实现密钥交换。

      2、使用DH算法：前提发送方和接受方协商使用同一个大素数P和生成数g，各自产生的随机数X和Y。发送方将g的X次方mod P产生的数值发送给接收方，接受方将g的Y次方mod P产生的数值发送给发送方，发送方再对接收的结果做X次方运算，接受方对接收的结果做Y次方运算，最终密码形成，密钥交换完成。

**六、同时实现数据的完整性、数据加密和身份验证所使用到的机制如下：**

   假设Bob和Rose进行通信：

          1】加密过程：

           Bob使用单向加密算法得出发送数据的特征码（用于数据完整性检测），Bob用自己的私钥加密此特征码（实现身份验证），并将此特征码置于数据的后面。Bob再生成一个密码D，用此密码加密加密过的特征码和数据（实现数据加密），此时生成的数据我们称其为Q，最后用Rose的公钥加密该密码D，并将D置于Q的后面。

          2】解密过程：

           Rose用自己的私钥解密得到D，然后用D解密得到数据和加密过得特征码，再用Bob的公钥解密此特征码，如果可以解密，则说明该数据是Bob发送的，反之，则不是。最后用单向加密算法计算该段数据的特征码，通过比较发送过来的特征码和Rose通过计算得到的特征码来确定此数据是否被篡改掉，如果特征码一致，则数据未发生改变；如果特征码不一致，则数据发生过改变。

**七、openssl：**

       1）组件：libcrypto:加密库。

                libssl：实现ssl功能的库。

                openssl：多用途的加密工具，能够提供对称加密、公钥加密、单向加密，且可以作为一个简单的本地CA用。

       2）在对称加密中，使用openssl实现对某个文件加密：

              openssl  enc  -des3  -salt  -a  -in  plaintext  -out  ciphertext.des3

          使用openssl实现解密：

              openssl  enc  -d  -des3  -salt  -a  -in  ciphertext.des3  -out  plaintext

       3）openssl version：查看openssl的版本信息。

       4）openssl ：进入openssl的命令行模式。

       5）openssl speed：测试某种加密算法加密不同长度密钥的速率。

       6）在公钥加密中，openssl可以用来生成私钥。

              openssl  genrsa 指定生成的私钥长度 > 保存到的文件名

              openssl  genrsa  [des3]  -out 保存到的文件名 指定生成的私钥长度

              在生成密钥文件的同时修改密钥文件的权限：（umask 077; openssl  genrsa 指定生成的私钥长度> 保存到的文件名）

              openssl  genrsa 指定生成的私钥长度 [-des3](加密私钥文件)  >  保存到的文件名。

              openssl  genrsa  [-des3]  -out  保存到的文件名  指定生成的私钥长度

              当私钥在生成的时候，文件未加密，则可以使用如下格式对未加密的私钥文件进行加密并保存：openssl  rsa  in  未加密私钥存放的文件 –des3  -out  保存到的文件名

   解密私钥：openssl  rsa  in  需要解密的私钥文件 –out  保存到的文件名。

       7）公钥在私钥中提取出：openssl  rsa  –in  my.key  -pubout 指定保存公钥的文件名。