文章编号:1005-8451(2003)06-0013-03

RSA 算法及其在电子商务中的应用

陈 风,张利萍

摘 要:在电子商务系统中,RSA 加密算法可以作为实现数据保密性和数据完整性的主要手段。叙述了如何在电子商务网站中,应用非对称加密算法 RSA 实现顾客个人信息的加密和数据完整性认证,讨论了加密算法所需的模幂算法的构造、素数和强素数的生成、数据加密和数字签名协议等关键技术,并给出具体算法。

关键词:RSA; 算法; 加密
中图分类号:TP39 文献标识码:A

RSA algorithm and it's application in e-Business

CHEN Feng, ZHANG Liping
(Computer Department of Beijing Institute of Technology, Beijing 100081)

Abstract: In e-Business System, RSA encryption algorithm can be the main method to implement data encryption and data integrity. It was discussed how to realize key technologies such as modular exponentiation , prime number construction ,strong prime number construction , encryption and digital signature protocol. Their detailed algorithms were given.

Keyword: RSA; algorithm; encryption

1 引言

在电子商务系统中,主要的安全技术要求有数据的保密性、数据的完整性和身份认证等。这几方面的要求都可以通过加密来实现:数据的保密性可以通过一定的加密算法对数据进行加密来保证,加密的数据在传送期间即使被截获也无法知道原文;数据的完整性可以通过对数据进行 Hash 函数的计算和数字签名来验证,Hash 函数可以采用不同的加密算法来产生;身份认证是为了确定通信双方的真实性等。文中叙述的主要是如何在电子商务网站中,应用非对称加密算法 RSA 实现顾客个人信息的加密和数据完整性认证,讨论了加密算法所需的模幂算法的构造、素数和强素数的生成、数据加密和数字签名协议等关键技术。

2 大数模幂运算快速算法的研究

RSA 算法涉及密集的模幂运算,最简单的模幂运算算法是二进制模幂运算,下面是从左到右的二进制模幂运算算法。

算法 1:从左到右的二进制幂运算

输出:$C=P^E \bmod M$

方法:
```
i=n-1;
C=1;
while i>=0 do {
    C=C*C mod M;
    if e_i=1 then C=C*P mod M;
    i=i-1;
        }
```

从左到右的二进制模幂运算每次都扫描一个比特位。以下,作者采用窗口法,每次扫描固定的比特位数,这一方法能大大提高模幂运算的效率。开窗口的过程是:从高位开始,扫描 w 位,为使每一个窗口的最高位为 1,规定在一个窗口后跳过所有连续的 0,直到遇到一个 1 再开下一个窗口。透过这些窗口,二进制序列中所有的 1 都露了出来。当开到最后一个窗口时,如果剩下的位数小于窗口的长度,则采用算法 1 的从左到右的二进制幂运算方法逐位处理,这样能保证除最后一个窗口外的所有窗口值都不小于 2^{w-1},从而能减少存储器的容量要求,当 w 较大时,效果更明显。下面是基于窗口法的快速模幂运算算法。

算法 2:基于窗口法的快速幂运算算法

输出:$C=P^E \bmod M$

预计算:

$R_0=1$;

收稿日期:2003-03-13

作者简介:陈 风,在读硕士研究生;张利萍,副教授。

```
R1=P;
i=2^(w-1);
Ri=P;
j=1;
    while j<=w-1 do      //预计算Ri=P^i mod M,i=2^(w-1)
      {
      Ri=Ri*Ri mod M;
      j=j+1;
     }
 while i<2^w-1 do      //预计算Ri=P^i mod M,(i=2^(w-1)+1,…2^w-1)
       {
       i=i+1;
       Ri=Ri-1*P mod M;
        }
方法二:
      S=en-1en-2…en-w;      //参数w为设定的窗口的大小
    C=Rs;
  i=n-w-1;
    while i>=0 do
        {
       C=C*C mod M;
       if ei=1 then
            {
        for j=1 to w-1 do C=C*C mod M;
        S=eiei-1…ei-w+1;
        C=C*Rs mod M;
       i=i-w+1;
       }
   i=i-1;
 if 0<=i<=w-2 then     //最后一个窗口需要特殊处理的判断
          {
          while i>=0 do
              {
            C=C*C mod M;
             if ei=1 then C=C*R1 mod M;
            i=i-1;
              }
           }
        }
```

3　素数和强素数的生成

素数是RSA算法的核心。素性检测的方法可以分为2大类:素性检测的概率方法和素性检测的非概率方法。素性检测的概率方法用得比较多,主要有:(1)Solovay—Strassen检测法,1977年。这是一种基于Jacobi符号来检测素性的概率方法。(2)Lehmann方法,1982年。(3)Rabin—Miller方法,1986年。文中主要介绍Rabin—Miller概率性方法,基于Rabin—Miller测试的素数生成算法如下:

算法3:

Step1.随机寻找一个大整数seed;

Step2.k←0;

Step3.n←seed + 2k;

Step4. 若n能通过B次Rabin-Miller测试,则转Step7.

Step5. k←k+1;

Step6. 若k>ln(seed),则转Step1, 否则转Step3;

Step7. n可能为素数,退出。

下面介绍强素数的生成。由研究,定义强素数p如下所示。

定义1:若素数p满足条件(1)或(2)时,则称p为强素数。

条件(1):p=2r+1,且r=s-1(mod s);

条件(2):p=1(mod r),且r=1(mod t), p=s-1(mod s);

其中r,s,t,p均为大素数。对于第一种情况,安全条件很强,下面是实现条件(1)的算法。

算法4:实现条件(1)

Step1. 调用算法3生成一个素数s;

Step2. 令r←2s+1;

Step3. 若r通过B次Rabin-Miller测试,则r是一个素数,转Step7;

Step4. 令r←r+2s;

Step5. 若r的二进制长度大于生成数p的长度,则转Step1;

Step6. 转Step3;

Step7. 令p←2r+1;

Step8. 若p通过B次Rabin-Miller测试,则p是一个强素数,转Step10;

Step9. 转Step1;

Step10. p是一个强素数,退出。

4　数据机密性和数据完整性的实现

数据机密性的实施就是对数据进行加密,以实现数据传输的安全性。数据完整性的实施就是对数据进行数字签名,以实现发送者身份和文档的认证。数据加密存在对称体制加密和非对称体制加密的区别,并且也存在一种数据加密的对称体制与非对称体制

结合的方法。数字签名的实施过程中用到的一种函数叫哈希函数（Hash 函数，单向散列函数），也有许多构造方法。假设有 Alice 和 Bob 进行通信，Bob 要确认信是 Alice 发出的。数字签名的基本协议很简单：

协议 1：

（1）Alice 用她的私人密钥对文件加密，从而对文件签名；

（2）Alice 将签名的文件传给 Bob；

（3）Bob 用 Alice 的公开密钥解密文件，从而验证签名。

在实际的实现过程中，明文 m 都是长文件，则上述第（1）步效率太低。为了节约时间，可以引入单向散列函数进行使用。Alice 并不对整个文件签名，而是对文件的散列值进行签名。下面介绍一种将 DES 算法和 RSA 算法结合起来的数据加密和数字签名协议：

协议 2：

（1）客户端和服务器建立一个连接；

（2）顾客进入个人信息加密网页；

（3）顾客申请服务器生成服务器的一个公钥和一个私钥；

（4）顾客生成顾客的一个公钥和一个私钥；

（5）顾客得到服务器的公钥后用它对一个会话密钥加密并传送给服务器；

（6）服务器用自己的私钥对加密了的会话密钥进行解密，得到会话密钥；

（7）顾客产生要传送文件 m 的单向散列值 h；

（8）顾客用他的私人密钥对单向散列值 h 进行加密得到数字签名 a；

（9）顾客用与服务器共享的会话密钥加密 m 和 a 并将结果传送给服务器；

（10）服务器用会话密钥解密这传送过来的信息，得到明文文件 m 和数字签名 a；

（11）服务器用明文文件 m 产生文件 m 的单向散列值 m'，同时用顾客的公钥对传过来的散列签名 a 进行解密，得到恢复的散列值。如果恢复的散列值与从 m 产生的散列值 m' 相同，则证明是顾客的签名。

以上算法和协议，作者都已编程实现。

5　结束语

一个安全的电子商务系统的实现，有赖于各方面的技术工作。但是，以上提到的技术是电子商务系统实现中的基本内容（即模幂、素数和强素数、数字加密和数字签名协议等）。文中给出了这些关键技术的解决方法，并加以编程进行了实现，因而奠定了一个成熟的电子商务系统能够实现的基础。

[参　考　文　献]

[1] 周芬, 高志强. 快速模幂算法及其硬件实现[J].微电子学, 2000, 30(6).

[2] Stephen E.Eldridge. Hardware Implementation of Montgomery's Modular Algorithm[J]. IEEE Transactions on Computers,1999, 42 (6).

·信息·

发挥信息化优势　提高货运经营效益

针对"非典"疫情造成旅客运输量下滑的情况，济南铁路局提出了"扩大货物运输，以货补客，增收节支"的重要措施。济南局电子中心急企业所急，充分发挥信息化优势，利用计算机网络技术，为夺取抗击"非典"和努力完成运输生产经营任务的双胜利提供现代化手段和强力支持。（1）完成路局货运调度管理信息系统的开发：该系统实时收集全局各车站、分局的货主请求信息，为路局领导提供准确、完整的货源状况。于 2003 年 5 月 16 日在路局货调系统投入使用。（2）开发货运装车方案优化管理信息系统：根据铁路局"高效货源全力确保，一般货源优化配置，低效货源灵活掌握"的发展方针，开展了货运装车计划方案优化管理信息系统的攻关。目前，系统的设计工作已经完成，进入编程阶段。预计 2003 年 6 月底能够投入使用。（3）完成"非典"疫情信息报告系统的开发：利用既有计算机网络，仅用一周时间完成局属单位"非典"疫情信息报告系统，于 2003 年 5 月 16 日正式运用。（4）完成"非典"防治监测网信息系统的开发：该系统已于 2003 年 5 月下旬正式在路局机关的处、室使用。下一步将在分局机关和具备综合局域网条件的大口、直属单位和基层站段推广。

文/本刊通讯员　宫树业