网络安全

本章重点

- 网络安全概述
- 对称加密和非对称加密
- 应用层安全——发送数字签名和数字加密的邮件
- 增加的安全套接字层
- 网络层安全 IPSec

信息安全主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、消息认证、数据加密等），直至安全系统，只要存在安全漏洞便可以威胁全局安全。

在本章，网络安全只专注于数据在传输过程中的安全，数据存储安全、操作系统安全等不在本章讨论范围。本章涉及到的安全有：应用层安全协议（比如发送数字签名的电子邮件，发送加密的电子邮件）、在传输层和应用层之间增加的安全套接字层（比如访问网站使用 https 协议）、在网络层实现的安全（IPSec）等，如图 10-1 所示。

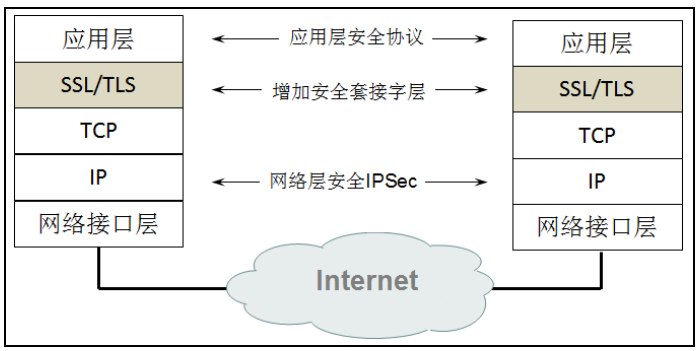

图 10-1　本章涉及到的网络安全

10.1 网络安全概述

本节讨论计算机网络面临的安全威胁和一般的数据加密模型。

10.1.1 计算机网络面临的安全威胁

计算机网络通信通常面临以下两大威胁，即主动攻击和被动攻击，如图 10-2 所示。

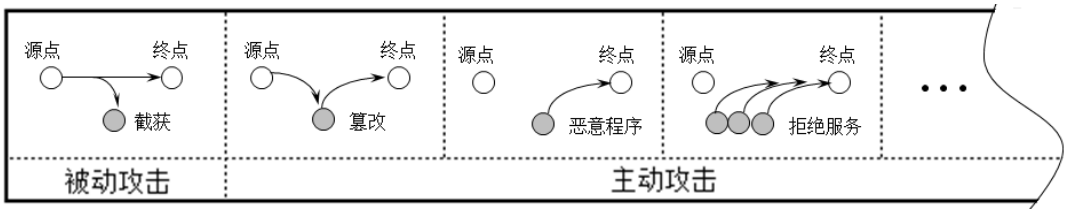

图 10-2 网络通信面临的威胁

（1）截获

攻击者从网络上窃听他人的通信内容，通常把这类攻击称为“截获”。在被动攻击中，攻击者只是观察和分析某一个协议数据单元 PDU（这里使用 PDU 这一名词是考虑到所涉及的可能是不同的层次）而不干扰信息流。即使这些数据对攻击者来说是不易理解的，他也可通过观察 PDU 的协议控制信息部分，了解正在通信的协议实体的地址和身份，研究 PDU 的长度和传输的频度，以便了解所交换的数据的某种性质。这种被动攻击又称为流量分析（traffic analysis）。

如图 10-3 所示，公司内网通过拨号服务器连接 Internet，内网计算机访问 Internet 的流量都要经过拨号服务器，如果在拨号服务器上安装抓包工具，就能捕获内网计算机上网流量。如果账号和密码是明文传输，那就危险了。当然，在拨号服务器上也可以安装流量分析软件，检测内网计算机上网流量和访问了哪些网站。这就是被动攻击。

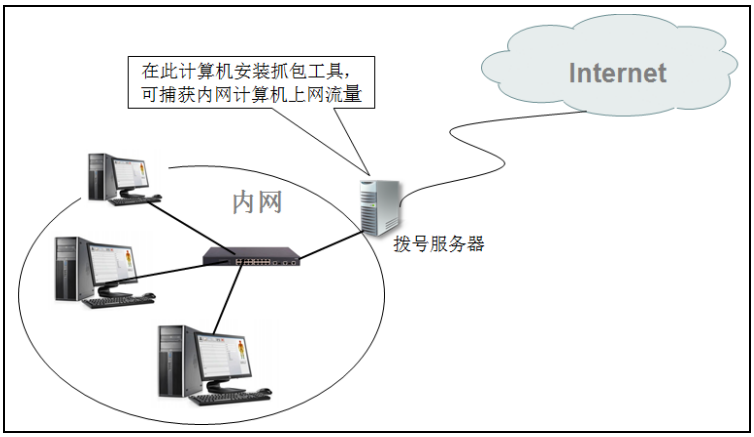

图 10-3 截获攻击示意图

（2）篡改

攻击者篡改网络上传送的报文。这里也包括彻底中断传送的报文，甚至把完全伪造的报文传送

给接收方，这种攻击方式有时也称为“更改报文流”。

DNS 劫持又称域名劫持，是十分常见的一种网络攻击手段，且轻易不被人察觉。用户用域名访问某个网站时，域名解析的响应报文被篡改，将解析到的 IP 地址修改成钓鱼网站的 IP 地址，让用户被钓鱼网站诈骗。

如图 10-4 所示，工商银行的网站 IP 地址是 113.207.33.16，域名是 www.icbc.com.cn，在因特网上有个假冒工商银行网站，该网站用来骗取用户的银行卡和密码，其 IP 地址是 23.20.12.18。

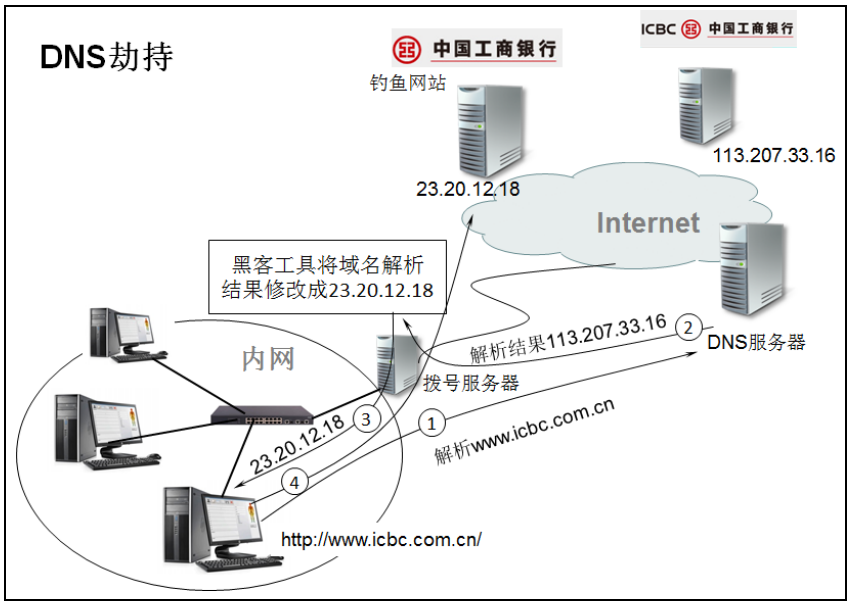

图 10-4　DNS 劫持示意图

如图 10-5 所示，在拨号服务器上安装一个黑客软件 Cain，配置该软件重写 www.icbc.com.cn 域名解析 DNS 响应包的 IP 地址为 23.20.12.18。

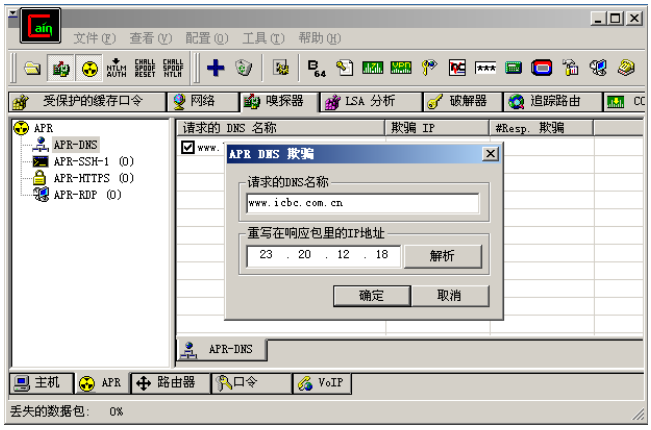

图 10-5　配置 ARP DNS 欺骗

内网计算机输入域名访问工商银行网站，域名解析的响应报文会被重写，将解析出的地址修改成 23.20.12.18 发送给内网计算机，内网计算机访问的是仿造的工商银行网站，而用户对此全然不知。

图 10-6 是在拨号服务器上捕获的内网计算机域名解析的数据包，第 15 个数据包是通过 Internet 上的 DNS 服务器解析 www.icbc.com.cn 域名的响应报文。大家可以查看解析的结果，该报文中的 IP 地址是工商银行网站的地址，多个 Web 服务器运行该网站，所以有多个 IP 地址。

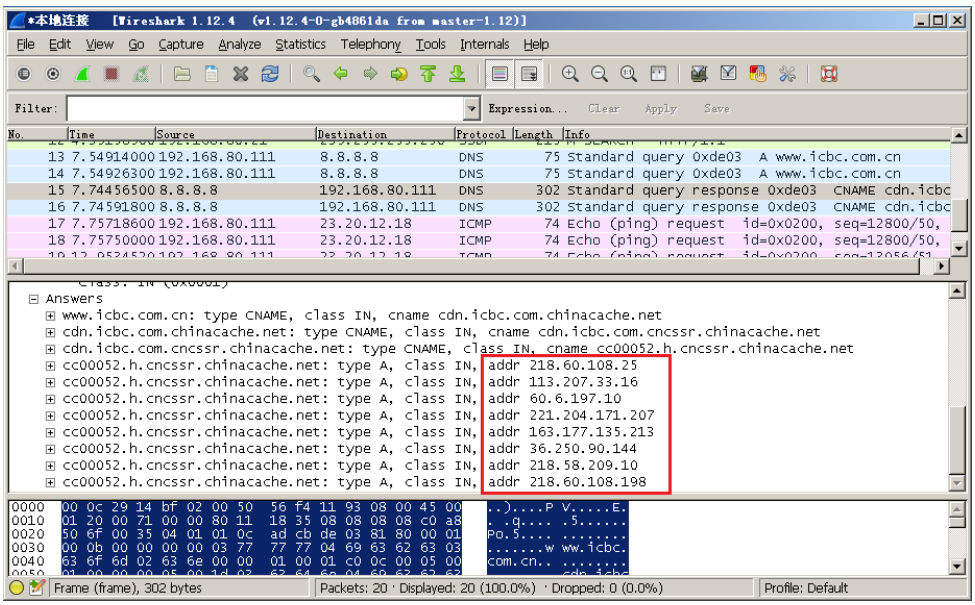

图 10-6　解析到的地址

如图 10-7 所示，第 16 个数据包是 Cain 软件修改第 15 个报文，产生新的 DNS 响应报文，把其中的 IP 地址都写成了 23.20.12.18。注意观察，只是修改了响应报文的内容，数据包的源地址和目标地址并没有改变，内网的计算机并不知道域名解析的响应报文被修改。

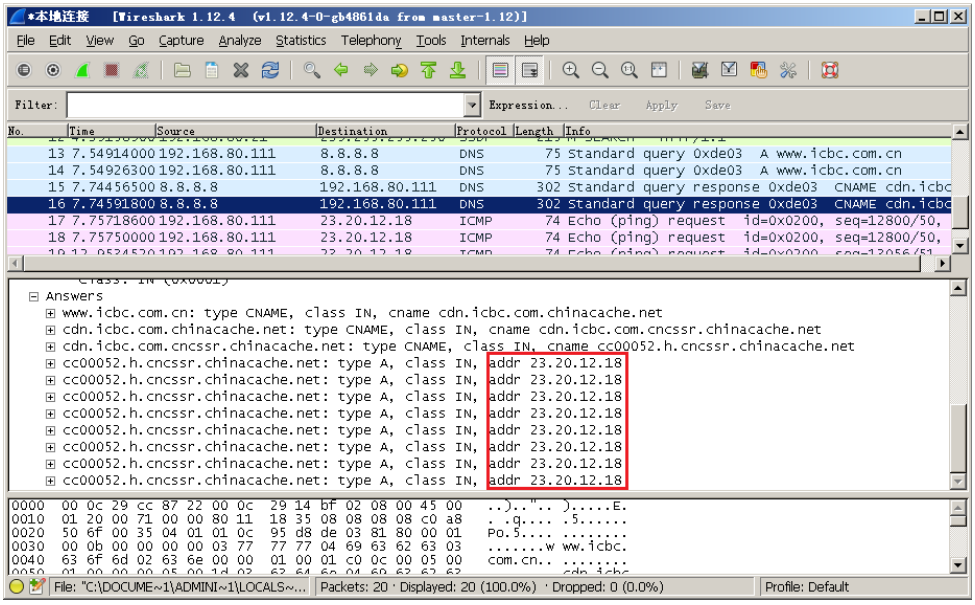

图 10-7　篡改解析的结果

DNS 劫持是篡改的一个应用，有很多高级防火墙（比如微软的 TMG 防火墙）可以直接修改 http 请求到的页面中的内容，完全可以把网页中的某些超链接替换成它指定的 URL。

（3）恶意程序

还有一种特殊的主动攻击就是恶意程序（rogue program）的攻击。恶意程序种类繁多，对网络安全威胁较大的主要有以下几种：

计算机病毒（computer virus），一种会“传染”其他程序的程序，“传染”是通过修改其他程序来把自身或其变种复制进去完成的。

计算机蠕虫（computer worm），一种通过网络的通信功能将自身从一个结点发送到另一个结点并自动启动运行的程序。

木马程序（Trojan horse program）通常称为木马、恶意代码等，是指潜伏在电脑中，与一般的病毒不同，它不会自我繁殖，也并不会“刻意”地去感染其他文件，是可受外部用户控制以窃取本机信息或者控制权的程序。它可以盗取 QQ 账号、游戏账号甚至银行账号，也可以用来远程控制或监控计算机（比如灰鸽子木马），或将本机作为工具来攻击其他设备等。计算机病毒有时也以特洛伊木马的形式出现。

逻辑炸弹（logic bomb）是一种当运行环境满足某种特定条件时执行其他特殊功能的程序。如一个编辑程序，平时运行得很好，但当系统时间为 13 日又为星期五时，就会删去系统中所有的文件，这种程序就是一种逻辑炸弹。

病毒是应用程序，病毒程序不会存储在交换机、路由器这些网络设备中，因此这些设备不会中病毒，但病毒可以通过交换机和路由器等网络设备传播到网络中其他计算机。计算机中了病毒也会影响网络设备的正常工作，比如有些病毒会在网络中发送大量 ARP 广播包，造成企业内网堵塞，还有些病毒每秒钟向 Internet 的某个地址建立几千个 TCP 连接，占用上网带宽。

（4）拒绝服务攻击

攻击者向因特网上的服务器不停地发送大量分组，使因特网或服务器无法提供正常服务，这种攻击被称为拒绝服务 DoS（Denial of Service）。若攻击者操纵因特网上的成百上千的网站集中攻击一个网站，则称为分布式拒绝服务 DDoS（Distributed Denial of Service）。有时也把这种攻击称为网络带宽攻击或连通性攻击。

有一种 DDoS 攻击叫做 CC（Challenge Collapsar，挑战黑洞）攻击，攻击者借助代理服务器生成指向攻击目标的合法请求，CC 主要是用来攻击网站。大家都有这样的经历，就是在访问论坛时，如果这个论坛比较大，并发访问的人比较多，打开页面的速度会比较慢。访问的人越多，网络流量就越高，造成网络堵塞，服务器系统资源就消耗越多，进而会引起服务器停止响应。CC 攻击就是操纵互联网上的成百上千个 Web 代理服务器，同时访问一个网站的 Web 页面，造成该网站停止响应或网络堵塞。

如图 10-8 所示，攻击者安装 CC 攻击工具，导入 Internet 上的 1500 个免费代理服务器，输入攻击目标 http://www.91xueit.com，点击“开始”，该软件就会向这 1500 个代理服务器发送请求，访问目标网站，这 1500 个代理服务器访问目标网站的流量汇聚到机房路由器，就会造成运营商机房网络堵塞，正常的访问将会被拒绝。

对于主动攻击，可以采用适当的措施加以检查。但对于被动攻击，通常是检测不出来的。根据这些特点，可得出计算机网络通信安全的目标如下：

- 防止析出报文内容和流量分析

- 防止恶意程序
- 检测报文流更改和拒绝服务

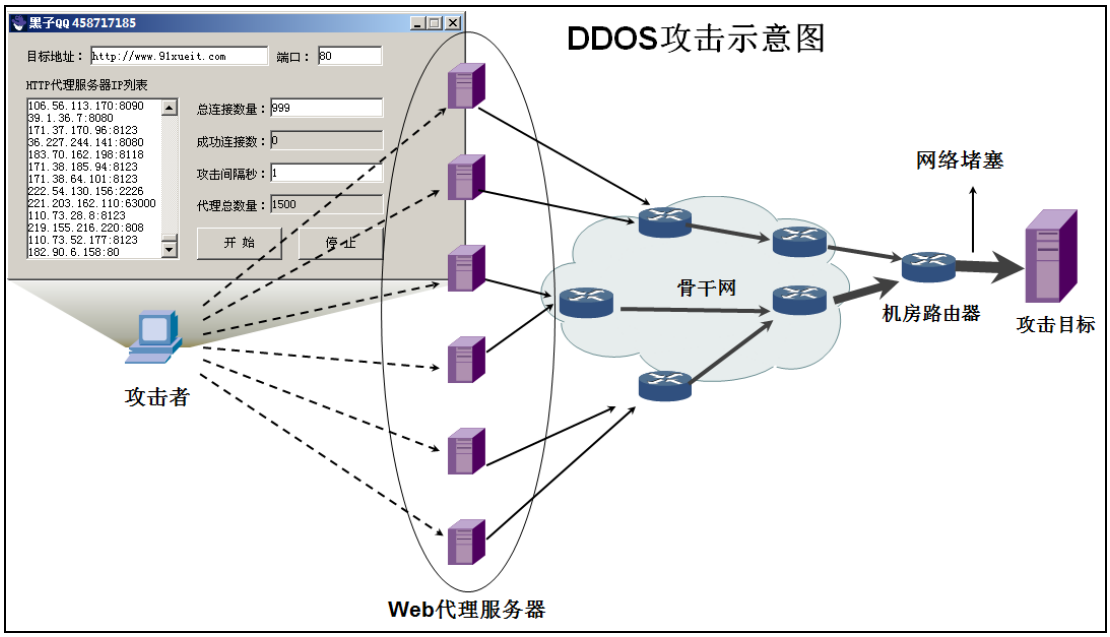

图 10-8　DDOS 攻击

对付被动攻击可采用各种数据加密技术，而对付主动攻击，则需要加密技术和适当的鉴别技术相结合。

10.1.2　一般的数据加密模型

一般的数据加密模型如图 10-9 所示。网络中的 A 计算机和 B 计算机打算进行加密通信，防止网络中的 C 计算机使用抓包工具抓包后查看 A、B 之间的通信内容。这就要求 A 发送前将数据加密后发给 B，在接收端 B 解密，得到明文。这需要事先预先协商好一个密钥 K，用户 A 向 B 发送明文 X，通过加密算法 E 运算后，就得出密文 Y。

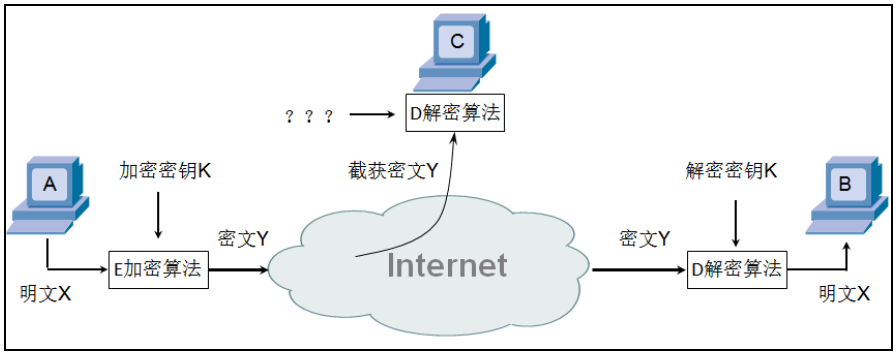

图 10-9　加密模型

图 10-9 中所示的加密和解密用的密钥 K（key）是一串秘密的字符串（或比特串）。明文通过

加密算法变成密文的一般表示方法为：

$$Y=E_K(X)$$

在传送过程中可能出现截取者（或攻击者、入侵者）。截取者即便知道解密算法，但是不知道解密密钥，亦没有办法解密得到明文 X。

接收端 B 使用解密算法 D 和解密密钥 K，解出明文 X。解密算法是加密算法的逆运算。在进行解密运算时如果不使用事先约定好的密钥就无法解出明文。解密运算表示为：

$$D_K(Y)=D_K(E_K(X))=X$$

如果加密密钥和解密密钥是同一个密钥，这种加密技术就称为“对称加密”。如果加密密钥和解密密钥不是同一个密钥，这种加密技术就称为“非对称加密”，但非对称加密的加密密钥和解密密钥有某种相关性。

密码编码学（cryptography）是密码体制的设计学，而密码分析学（cryptanalysis）则是在未知密钥的情况下从密文推演出明文或密钥的技术。密码编码学与密码分析学合起来即为密码学（cryptology）。

如果不论截取者获得了多少密文，但在密文中都没有足够的信息来唯一地确定出对应的明文，则这一密码体制称为无条件安全的，或称为理论上不可破的。在无任何限制的条件下，目前几乎所有实用的密码体制均是可破的。因此，人们关心的是要研制出在计算上（而不是在理论上）不可破的密码体制。如果一个密码体制中的密码不能在一定时间内被可以使用的计算资源破译，则这一密码体制称为在计算上是安全的。

10.2 对称加密和非对称加密

10.2.1 对称密钥密码体制

所谓对称密钥密码体制，即加密密钥与解密密钥是相同的密码体制。

数据加密标准 DES 属于对称密钥密码体制。它由 IBM 公司研制，于 1977 年被美国定为联邦信息标准后，在国际上引起了极大的重视。ISO 曾将 DES 作为数据加密标准。

DES 是一种分组密码。在加密前，先对整个明文进行分组。每一个组为 64 位长的二进制数据。然后对每一个 64 位二进制数据进行加密处理，产生一组 64 位密文数据。最后将各组密文串接起来，即得出整个密文。使用的密钥为 64 位（实际密钥长度为 56 位，有 8 位用于奇偶校验）。

DES 的保密性仅取决于对密钥的保密，而算法是公开的。目前较为严重的问题是 DES 的密钥长度。56 位长的密钥意味着共有 2^{56} 种可能的密钥，也就是说，共约有 2^{56} 种密钥。假设一台计算机 1μs 可执行一次 DES 加密，同时假定平均只需搜索密钥空间的一半即可找到密钥，那么破译 DES 要超过 1000 年。

但现在已经设计出搜索 DES 密钥的专用芯片。例如在 1999 年有一批人在因特网上合作借助于一台不到 25 万美元的专用计算机，在略大于 22 小时的时间就破译了 56 位密钥的 DES。若借助价格为 100 万美元或 1000 万美元的机器，则预期的搜索时间分别为 3.5 小时或 21 分钟。

在 DES 之后又出现了国际数据加密算法 IDEA（International Data Encryption Algorithm）。IDEA 使用 128 位密钥，因而更不容易被攻破。计算指出，当密钥长度为 128 位时，若每微秒可搜索一百万次，则破译 IDEA 密码需要花费 5.4×10^{18} 年。这显然是比较安全的。

在对称加密算法中常用的算法有：DES、3DES、TDEA、Blowfish、RC2、RC4、RC5、IDEA、SKIPJACK、AES 等。

对称加密算法的优点是算法公开、计算量小、加密速度快、加密效率高。

对称加密算法的缺点是在数据传送前，发送方和接收方必须商定好密钥，然后使双方都能保存好密钥；其次如果一方的密钥被泄露，那么加密信息也就不安全了。另外，每对用户每次使用对称加密算法时，都需要使用其他人不知道的唯一密钥，这会使得收、发双方所拥有的钥匙数量巨大，密钥管理成为双方的负担。如果企业内用户有 n 个，则整个企业共需要 n×(n-1)/2 个密钥，密钥的生成和分发将成为企业信息部门的恶梦。

10.2.2 公钥密码体制

公钥密码体制（又称为公开密钥密码体制）的概念是由斯坦福（Stanford）大学的研究人员 Diffe 与 Hellman 于 1976 年提出的。公钥密码体制使用不同的加密密钥与解密密钥，故称为非对称加密。

非对称加密算法需要两个密钥来进行加密和解密，这两个密钥是公开密钥（public key，简称公钥）和私有密钥（private key，简称私钥），且不能通过公钥推算出私钥。公开密钥与私有密钥还必须成对使用，如果用公开密钥对数据进行加密，那么只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。

下面举例说明公钥密码体制的加密和解密过程。如图 10-10 所示，A 要给 B 发送加密数据，第一步是 B 产生一个密钥对（B 的公钥 PK_B 和 B 的私钥 SK_B）。B 将公钥 PK_B 通过网络传给 A。假如在此过程网络中的 C 截获了 B 的公钥 PK_B。

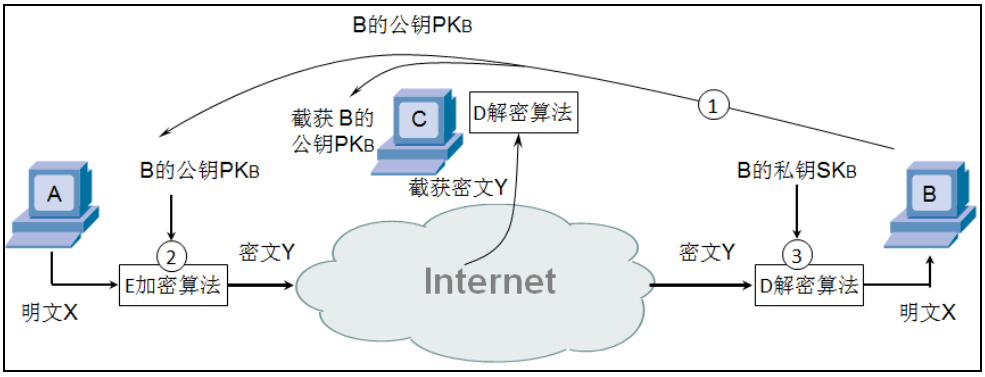

图 10-10　非对称加密

A 使用 B 的公钥 PK_B 加密明文，得到密文 Y，发送给 B。

C 捕获密文 Y，使用前面截获的 B 的公钥 PK_B，不能解密出明文（公钥加密必须用私钥才能解密），即便知道解密算法也无济于事。

密文 Y 到达 B，使用 B 的私钥 SK_B 解密得到明文 X。B 的私钥千万不能泄露，否则其他人也可以解密发给他的信息了。

非对称加密与对称加密相比，其安全性更好：对称加密的通信双方使用相同的密钥，如果一方的密钥遭泄露，那么整个通信就会被破解。而非对称加密使用一对密钥，一个用来加密，一个用来解密，而且公钥是公开的，密钥是自己保存的，不需要像对称加密那样在通信之前要先同步密钥。

非对称加密的缺点是加密和解密花费时间长、速度慢，只适合对少量数据进行加密。

在非对称加密中使用的主要算法有：RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）等。

请注意，任何加密方法的安全性取决于密钥的长度，以及攻破密文所需的计算，而不是简单地取决于加密的体制（公钥密码体制或传统加密体制）。我们还要指出，公钥密码体制并没有使传统密码体制成为陈旧过时的，因为目前公钥加密算法的开销较大，在可见的将来还看不出要放弃传统的加密方法。

10.2.3 非对称加密细节

对称加密算法的优点是算法公开、计算量小、加密速度快、加密效率高。但密钥在网络中传输存在被截获的风险。而非对称加密，公钥可以在网络中传输，不用担心被截获，但非对称加密和解密花费时间长、速度慢，只适合对少量数据进行加密。

如何将这两种加密技术的优点相结合呢？

如图 10-11 所示，A 给 B 发送一个 500M 大小的文件，如果使用 B 的公钥 PK_B 直接加密这么大的文件，耗时较长而且效率不高。A 产生一个对称密钥，比如“123abc”，使用该对称密钥加密 500M 的文件，虽然文件很大，但对称加密效率高，很快完成。加密完成后，再使用 B 的公钥加密对称密钥“123abc”，虽然非对称加密效率低，但加密这个对称密钥还是很快的。

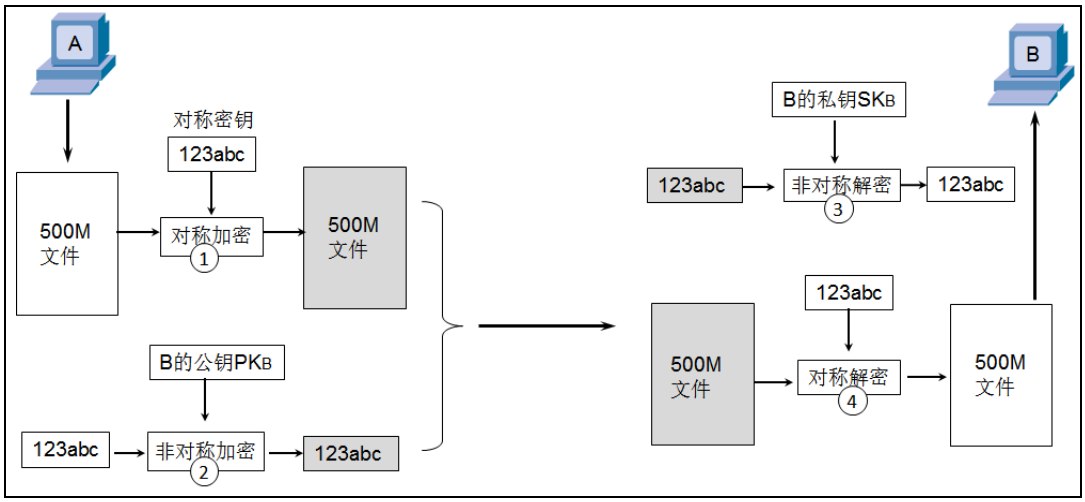

图 10-11 非对称加密细节

A 把加密后的 500M 文件和加密后的对称密钥一起发给 B，B 收到后，使用 B 的私钥 SK_B 解密得到对称密钥“123abc”，然后再使用“123abc”解密这 500M 的文件，效率很高。

这种方式就利用了对称加密、解密速度快，效率高的优点，也利用了非对称加密，公钥可以在网上传输的优点。

上面讲的是非对称加密的细节，很多应用程序都在使用非对称技术加密数据时，结合应用了对称加密技术。

10.2.4 数字签名细节

非对称加密还可以用来实现数字签名，在讲数字签名之前，先想一想你是否找领导签过字呢？

找领导签字的目的和意义是什么呢？

比如我要去北京参加一个会议，要预支差旅费，找财务填写了一个差旅申请表，填写好申请人、出差目的、地点、时间，最关键的是领取差旅费的金额，填写好了，找到主管领导签字后，就可以去财务领取差旅费了。

如果领导看到这个月的财务报表，发现差旅费高于其他月份，就要问财务什么情况，财务人员就可以拿出由他签字的差旅申请单，他就无话可说了。有领导的签字，他就不能抵赖，说他不知道这回事。

大家再想想，如果我填写差旅申请单，领取差旅费金额的那一栏不填写就找领导签字，他会同意么？如果他先填写“同意”，签了他的名字。我要随意填写差旅费金额，去财务领钱，怎么办？因此领导在签名前一定认真查看所有的内容，确保完整无误，才敢签名。签名之后就不能再更改其中的内容，如果财务人员看到涂改过的差旅申请单，虽然有领导签字，还会让你重填一份，找领导签字。

这是在工作中领导签名的意义：

（1）有你的签名，你就不能抵赖，说你没有看过这个文件。

（2）签名后，就不允许更改文件中的内容。

在互联网中的数字签名也是为了实现以上两个目的，保证信息传输的完整性、发送者的身份认证和防止抵赖发生。

数字签名如何实现呢？

如图 10-12 所示，A 要发送一个数字签名的文件给 B，这要求 A 有一个密钥对（A 的私钥 SK_A 和 A 的公钥 PK_A）。使用哈希函数生成该文件的摘要，再使用 A 的私钥 SK_A 加密摘要（这个过程叫做签名，私钥持有者才能做这个操作）。然后将加密后的摘要、A 的公钥 PK_A 和文件（不加密该文件）一起发送给 B。

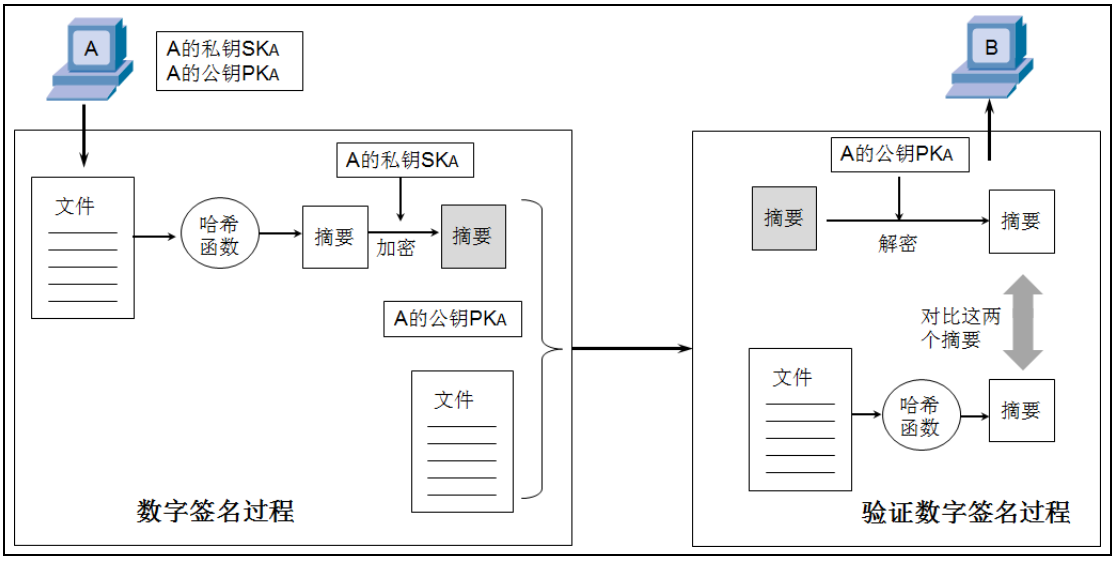

图 10-12　数字签名的细节

B 收到后，就要验证该文件在传输过程中是否被更改、数字签名是否有效。B 将加密的摘要使

用 A 的公钥 PK_A 解密得到一个摘要，B 将收到的文件通过哈希函数生成一个摘要，比较这两个摘要，如果一样，就认为 A 签名有效。

> 哈希函数又称单向散列函数，指的是根据输入消息（任何字节串，如文本字符串、Word 文档、JPG 文件等）输出固定长度数值的算法，输出数值也称为“散列值”或“消息摘要”，其长度取决于所采用的算法，通常在 128 ~ 256 位之间。单向散列函数旨在创建用于验证消息完整性的简短摘要。

总结，数字签名有两种功效：一是能确定消息确实是由发送方签名并发出来的，因为别人假冒不了发送方的签名；二是数字签名能确定消息的完整性，因为数字签名的特点是它代表了文件的特征，文件如果发生改变，数字摘要的值也将发生变化，不同的文件将得到不同的数字摘要。

10.2.5 数字证书颁发机构（CA）

在互联网中，通信双方的计算机自己生成密钥对，将公钥出示给对方来验证自己的签名，接收方依然很难断定对方的身份。这就和我们的身份证一样，如果我们可以自己造身份证，在身份证随意填写个人信息，你向其他人出示自己造的身份证，没人相信。当你出示公安局颁发的身份证时，其他人就相信你身份证的信息是真实的。其他人不相信你，但相信公安局，相信公安局给你发证时已经核实了你的身份信息。

在互联网上进行交易的企业或个人，他们使用的密钥对也要由专门机构发放，在计算机中这些密钥对是以数字证书的形式出现的，数字证书还包含了使用者的个人信息、发证机构。

电子商务认证授权机构（CA，Certificate Authority）也称为电子商务认证中心，是负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。

比如 http://www.sheca.com/是上海数字证书认证中心网址，http://www.hebca.com/是河北省电子认证有限公司网址，如图 10-13 所示。我们可以向这些机构申请证书，证书到期了，可以更新证书，证书丢失了，可以吊销证书。

图 10-13　河北省 CA

下面是向河北省电子认证有限公司申请证书的流程。需要选择应用领域和证书类型，填写新办数字证书申请表，支付费用，携带证明材料领取数字证书（这一点很重要，就是核实申请人身份）。

1．选择应用领域及证书类型

选择所申请数字证书使用的领域及证书类型。

2．填写新办数字证书申请表

点击“新办证书业务办理”按钮，填写《新办数字证书申请表》，提交成功后请牢记申请表受理编号，以便查询新办证书业务办理情况。如果您已经填写过《新办数字证书申请表》，请点击“查询新办证书业务办理情况”按钮，查询办理进度。

3．支付数字证书新办费用

如尚未交费，请在填表后的支付页面支付数字证书新办费用。
支付方式：1.网上支付 2.银行电汇
账户信息如下：
账户名称：河北省电子认证有限公司
账号：13001615608050509388
开户银行：中国建设银行石家庄红旗大街支行
行号：105121061113

4．携带证明材料领取数字证书

自付款成功的第二个工作日起，请携带以下材料到河北 CA 通知的证书办理地点或河北 CA 当地办事处领取证书：
1）组织机构代码证副本复印件，加盖公章；
2）营业执照副本复印件，加盖公章；
3）经办人身份证原件及复印件，加盖公章；
4）打印好的新办单位证书申请表，加盖公章。

10.2.6 使用 CA 颁发的证书数字验证签名的过程

本节讲解使用 CA 颁发的证书进行签名和验证数字签名的过程。

如图 10-14 所示，证书颁发机构先要给自己生成一个密钥对，CA 的私钥和 CA 的公钥，以后给用户或企业颁发数字证书时，都用 CA 的私钥进行签名。网络中的用户或企业只要信任这个证书颁发机构，也就是有 CA 的公钥，就可以使用 CA 的公钥验证别人出示的证书是不是这个 CA 颁发的，如果验证通过，也就能够相信这个证书上的信息是真实的，确实有这样的一个人或企业。

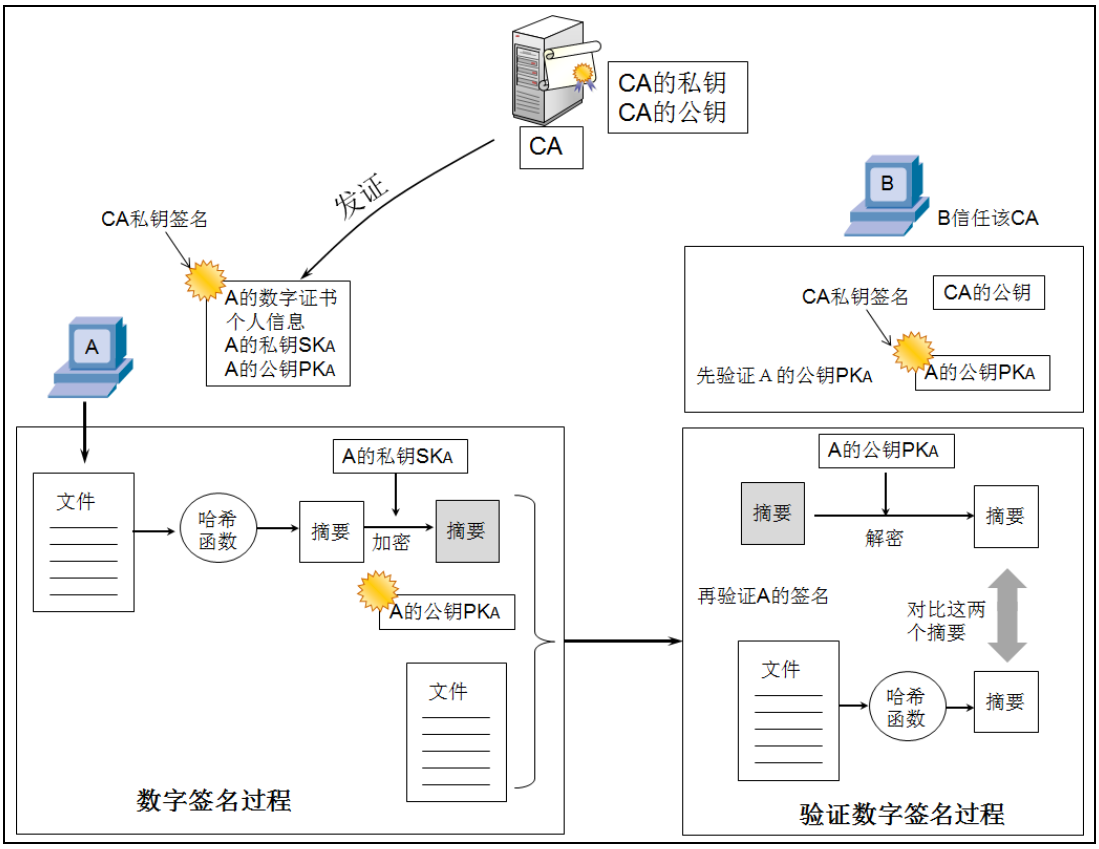

图 10-14 使用 CA 颁发的证书验证数字签名的过程

A 向 CA 提交证书申请，CA 核实 A 提交的信息，为 A 产生一个数字证书，该数字证书包含 A 的个人信息、A 的私钥、A 的公钥还有证书颁发者等信息，该证书用 CA 的私钥签名。

A 得到的数字证书包含 A 的私钥和 A 的公钥，可以从该证书中单独导出 A 的公钥，当然该公钥也有 CA 的数字签名。

A 给 B 发送一个数字签名的文档，这时 B 首先要做的是核实 A 的身份，验证 A 出示的证书（只有公钥）是否是 CA 颁发的。这时 B 计算机必须有 CA 的公钥，使用 CA 的公钥验证 A 证书是否来自 CA。验证通过后，再使用 A 的公钥验证其签名的文件。

这样 A 和 B 虽然都是网络中的个人或企业，互不信任，没办法知道对方的身份，只要 A 出示的证书是 B 信任的证书颁发机构颁发的，B 就可以使用该证书颁发机构的公钥验证 A 出示的证书（公钥）是否来自该 CA，然后再使用 A 出示的证书（公钥）验证其数字签名的文件。

10.3 实战：发送数字签名和数字加密的邮件

前面讲了公钥密码体系可以用来加密和数字签名。下面就来体验一下如何在 WindowsServer2003 上安装证书颁发机构、在 WindowsXP 上申请电子邮件证书，发送数字签名的邮件和加密的邮件。

本节的实验环境需要三个虚拟机，如图 10-15 所示，WindowsServer2003 安装 CA 服务，

WindowsXP1 配置 Outlook Express 连接搜狐的邮件服务器收发电子邮件，邮箱账户为 dongqing91@sohu.com，WindowsXP2 配置 Outlook Express 连接搜狐的邮件服务器收发电子邮件，邮箱账户为 dongqing081@sohu.com。

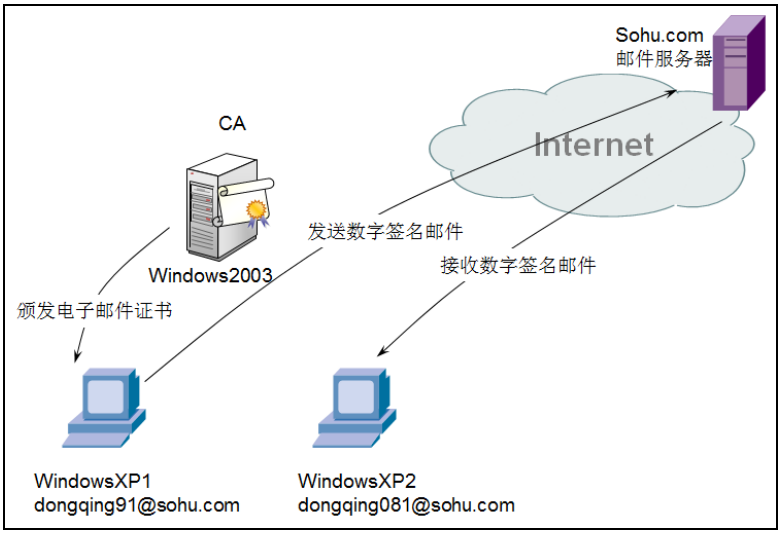

图 10-15　发送数字前的邮件

10.3.1　安装证书颁发机构

向互联网上的认证机构申请数字证书需要提交资料、支付费用。要只是单纯为了学习，体验一下数字签名、数字加密的用法，就没必要去这些机构申请数字证书了。我们在 WindowsServer2003 安装证书颁发机构，就可以为其他人颁发数字证书了，不过向 Internet 上的用户出示你自己的 CA 颁发的证书，他们是不会信任的，不过在一个范围内使用是没问题的，比如你可以让内部员工信任企业部署的 CA。

如图 10-16 所示，在 Windows2003CA 虚拟机安装 Windows 组件，选中“应用程序服务器”和“证书服务”，点击“下一步”。因为用户需要通过访问证书颁发机构的网站申请证书，所以要安装应用程序服务器（也就是安装 IIS 服务）。

如图 10-17 所示，在出现的“CA 类型”对话框中选中“独立根 CA”，点击“下一步”。这个过程会生成 CA 证书。

> 独立 CA 和企业 CA 的区别：
>
> CA 可以面向开放用户颁发证书，例如大型商用 CA 专门向互联网数以百万计的用户和服务器发放证书，这叫做独立 CA。互联网上的用户申请证书时，CA 需要核实申请者的信息真实性，然后颁发。安装独立 CA 的服务器可以是域中的成员也可以是工作组中的服务器。
>
> 企业内部也可以安装自己的 CA，这叫做企业 CA。企业 CA 为企业内的用户和计算机发放数字证书。企业 CA 利用 Active Directory（活动目录）确定请求者的身份，并确定请求者是否具有请求特定证书类型所要求的安全性权限。如果只为公司内部的用户和计算机发放证书，就应该建立一个企业 CA。

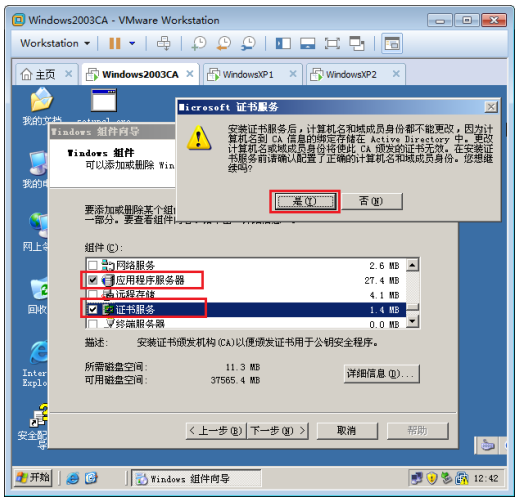

图 10-16　安装证书服务

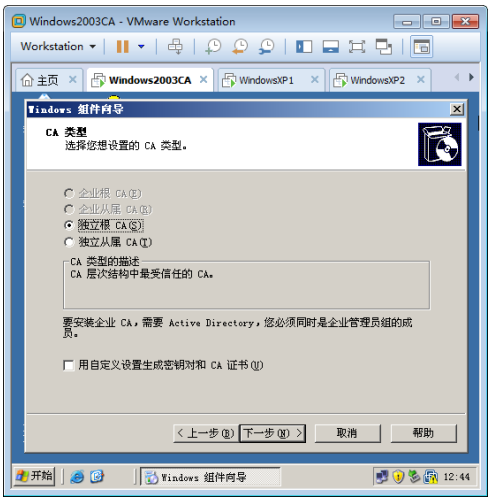

图 10-17　选择证书类型

如图 10-18 所示，在出现的“CA 识别信息”对话框中输入 CA 的公用名称，证书有效期默认 5 年，点击“下一步”。

如图 10-19 所示，在出现的“证书数据库设置”对话框中指定证书数据库路径和证书数据库日志路径，点击“下一步”。

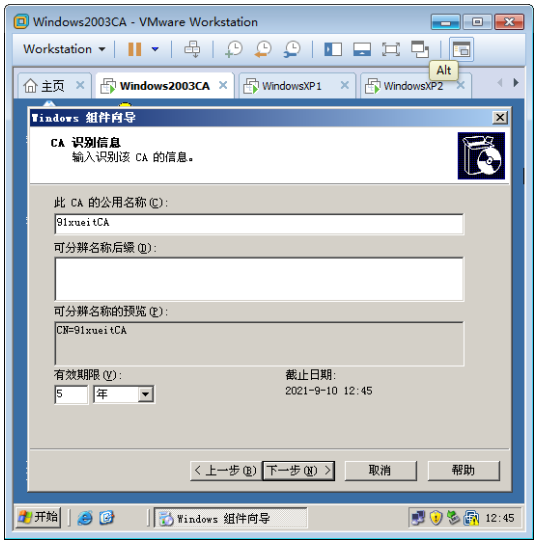

图 10-18　指定 CA 名称

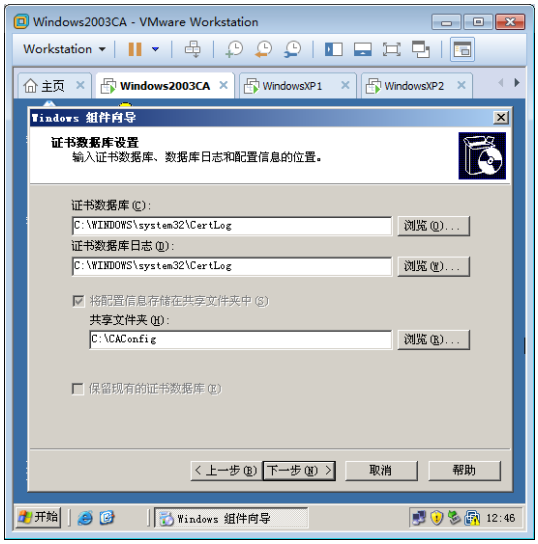

图 10-19　证书数据库位置

如图 10-20 所示，在安装过程中会出现 Microsoft 证书服务提示，提示要启用 ASP 模块，点击“是”。

如图 10-21 所示，安装完成后，点击“开始”→“程序”→“管理工具”→“证书颁发机构”，打开证书颁发机构管理工具。

如图 10-22 所示，打开“Internet 信息服务（IIS）管理器”窗口，可以看到默认网站下有一个虚拟目录 CertSrv，网络中的计算机通过访问默认网站的该目录申请数字证书。

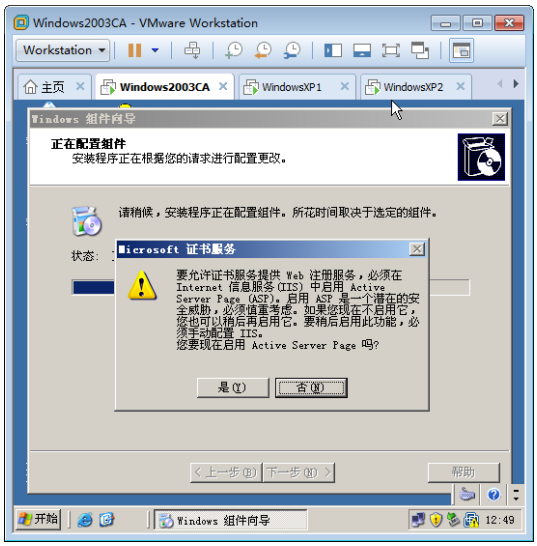

图 10-20　完整启用 ASP

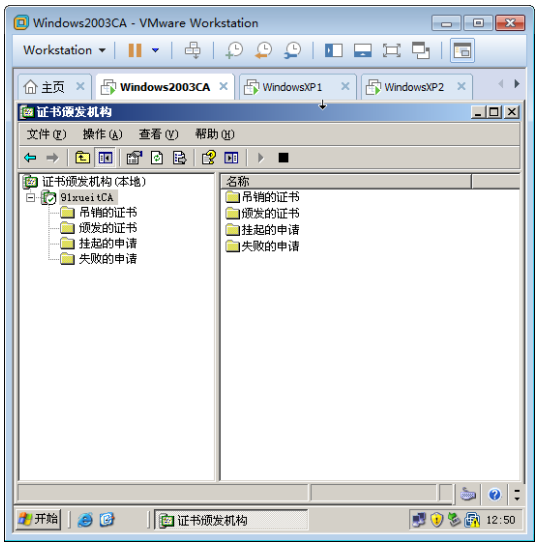

图 10-21　打开证书管理工具

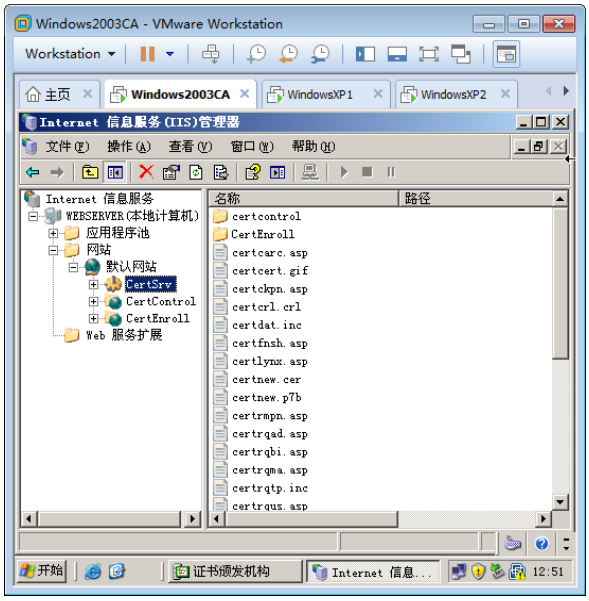

图 10-22　申请证书的网站

10.3.2　申请和颁发电子邮件数字证书

在 Windows XP 上申请电子邮件证书，向证书颁发机构申请证书，你首先要信任该证书颁发机构，就是将 CA 的公钥添加到受信任的根证书颁发机构。

如图 10-23 所示，输入 http://192.168.80.10/certsrv/，在出现的网页中点击“下载一个 CA 证书，证书链或 CRL”。

如图 10-24 所示，在出现的新页面中点击“安装此 CA 证书链”，在出现的提示对话框中点击“是”。

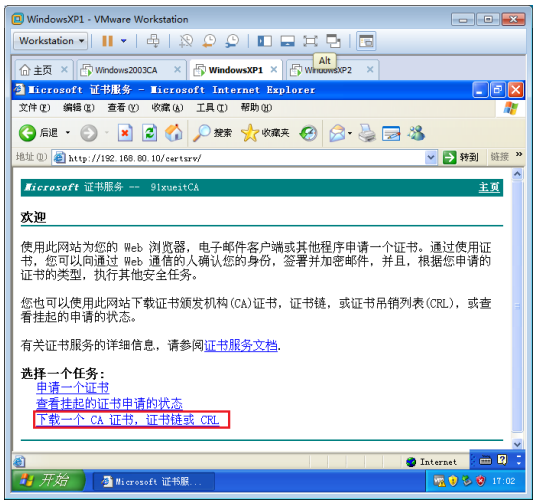

图 10-23　下载 CA 公钥

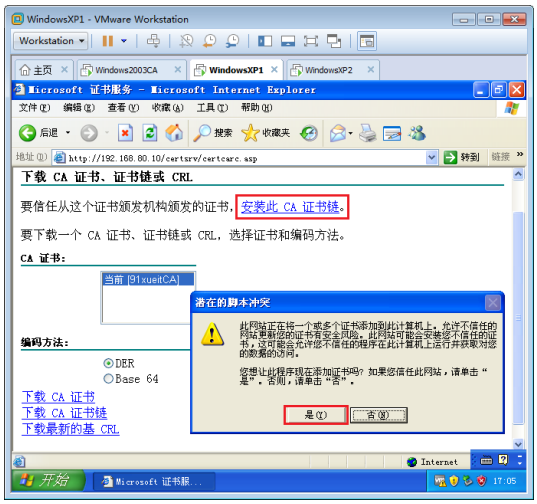

图 10-24　安装 CA 证书

如图 10-25 所示，在出现的安全警告对话框中点击“是”。安装完成后，点击浏览器“开始”→“Internet 选项”。

如图 10-26 所示，在出现的“Internet 选项”对话框的“内容”选项卡下，点击“证书”。

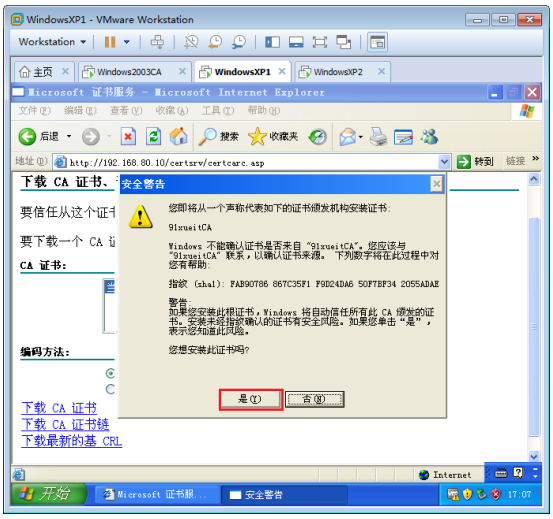

图 10-25　信任证书颁发机构

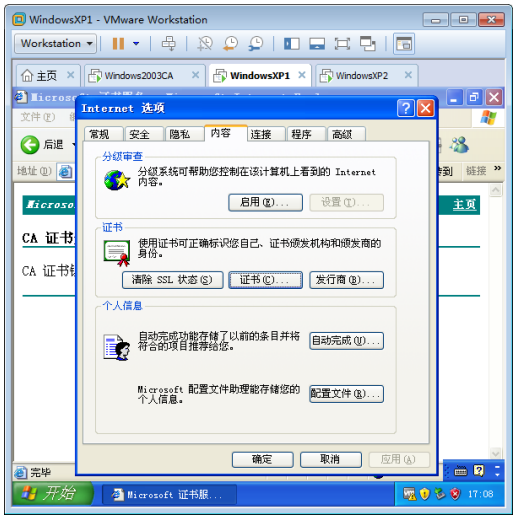

图 10-26　查看证书

如图 10-27 所示，在出现的“证书”对话框的“受信任的根证书颁发机构”选项卡下，可以看到已经出现了 91xueitCA，这就意味着当前用户已经信任了该证书颁发机构，有了该证书颁发机构的公钥。

注意：证书分为计算机证书和用户证书，用户只能管理自己的证书和信任的证书颁发机构，A 用户信任的证书颁发机构 B 用户不一定信任。计算机证书只有计算机管理员能够管理，不依赖登录的用户。

如图 10-28 所示，返回主页，点击“申请一个证书”。

如图 10-29 所示，在出现的“申请一个证书”页面中点击“高级证书申请”。

如图 10-30 所示，在出现的“高级证书申请”页面中点击“创建并向此 CA 提交一个申请”。

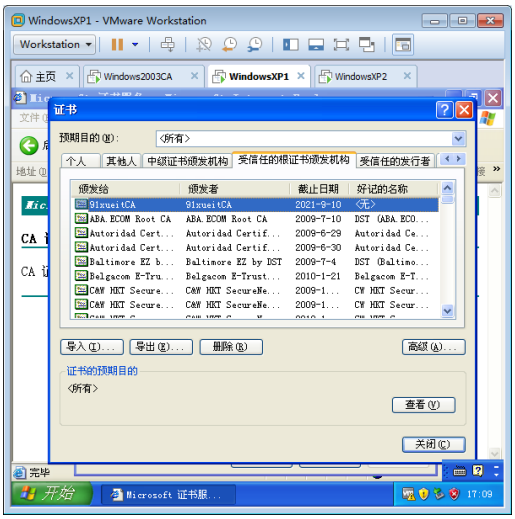

图 10-27　查看用户信任的根证书颁发机构

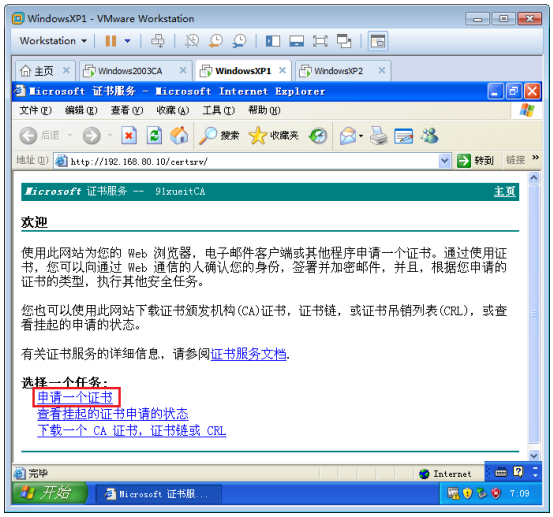

图 10-28　申请证书

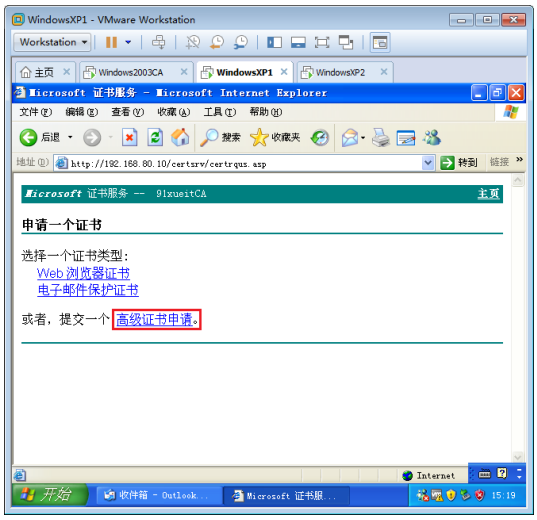

图 10-29　高级申请

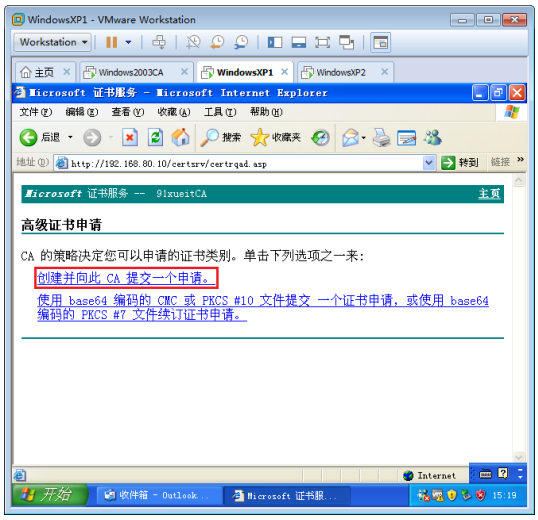

图 10-30　创建提交申请

如图 10-31 所示，在出现的“高级证书申请”对话框中输入识别信息：姓名、电子邮件、公司、部门，中国就写 cn。

这里填写的信息不要有中文，且电子邮件地址一定要和 Outlook Express 配置的电子邮箱一样，否则 Outlook Express 邮箱账户不能使用该数字证书。

如图 10-32 所示，选择需要的证书类型“电子邮件保护证书”，选中“标记密钥为可导出”。

选中“标记密钥为可导出”，用户以后就可以从计算机导出证书（包含公钥和私钥）进行备份，否则以后只能导出证书（只包含公钥），这样用户重装系统，或从另一台计算机收邮件，就不能使用证书了。

如图 10-33 所示，其他选项保持默认，输入好记的名称，点击“提交”。

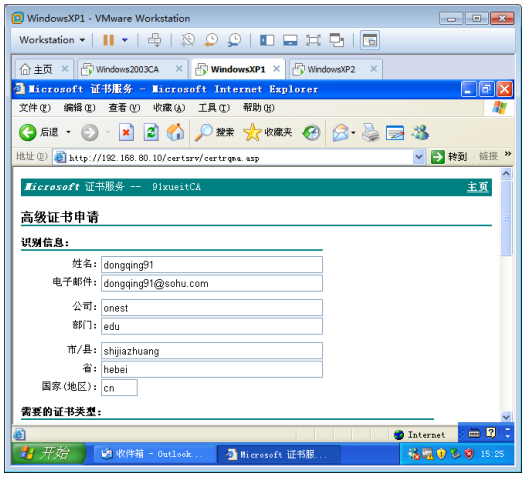

图 10-31　输入个人信息

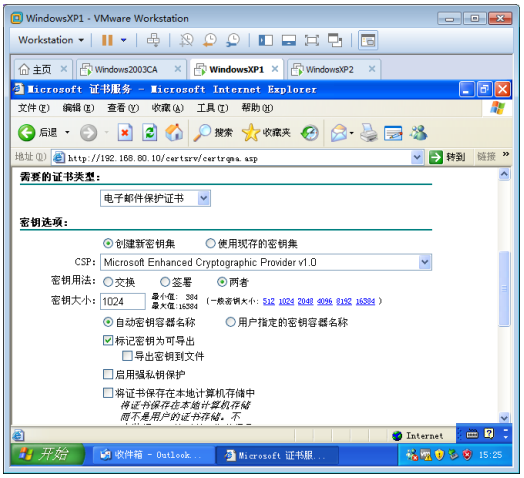

图 10-32　指定证书选项

如图 10-34 所示，在 Windows2003CA 上，选中“挂起的申请”，在右侧可以看到刚刚提交的申请，右击该申请，点击“所有任务”→“颁发”。

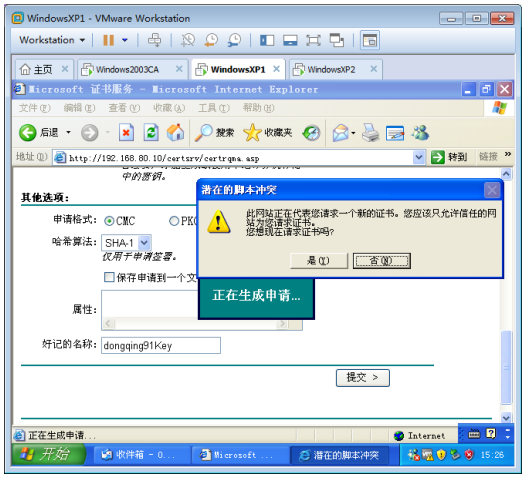

图 10-33　提交申请

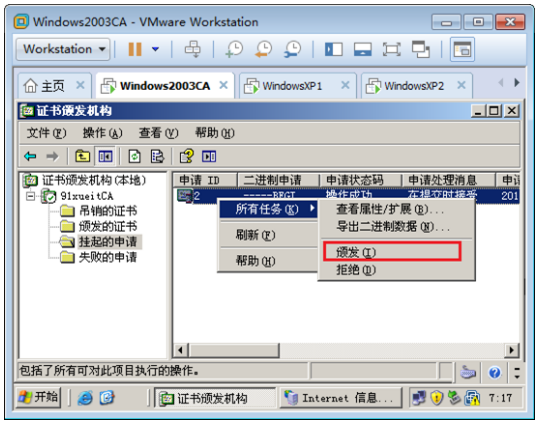

图 10-34　颁发证书

如图 10-35 所示，在 WindowsXP1 上，返回申请数字证书的首页，点击“查看挂起的证书申请的状态”。

如图 10-36 所示，在出现的“查看挂起的证书申请的状态”页面，能够看到已经颁发的数字证书，点击申请的“电子邮件保护证书”。

如图 10-37 所示，可以看到申请的证书已颁发，点击“安装此证书”，在出现的“潜在的脚本冲突”对话框中点击“是”。

如图 10-38 所示，打开“Internet 选项”对话框，再次查看证书，在“个人”选项卡下，可以看到刚才安装的证书，下面有导入、导出按钮，在这里我们点击“查看”。

如图 10-39 所示，在出现的“证书”对话框的“常规”选项卡，可以看到证书信息：证书目的、颁发者、颁发给、有效期，还能看到“您有一个与该证书对应的私钥”。

如图 10-40 所示，在“详细信息”选项卡下，可以看到有效期、主题（使用者的信息）等信息。

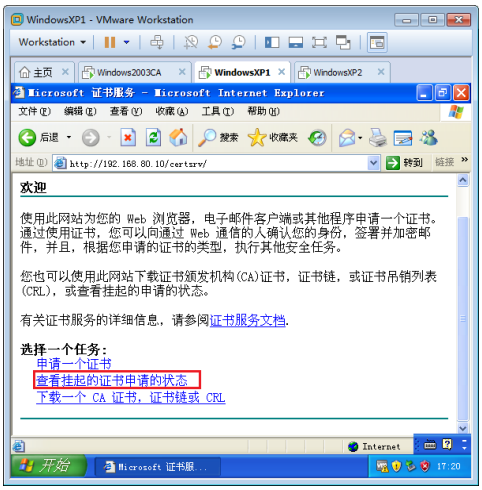

图 10-35　查看申请的证书

图 10-36　看到颁发的证书

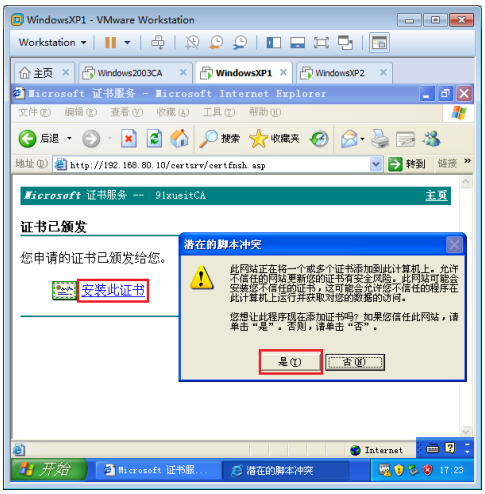

图 10-37　安装数字证书

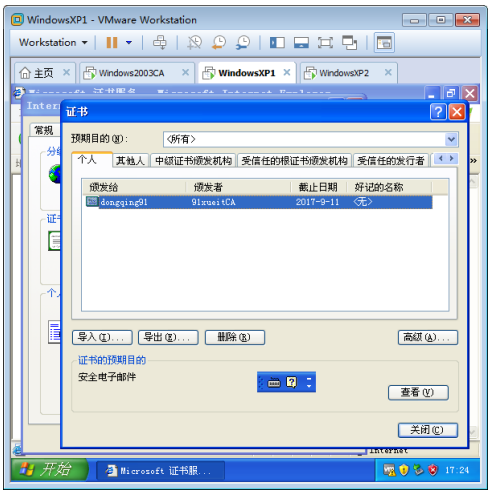

图 10-38　查看用户证书

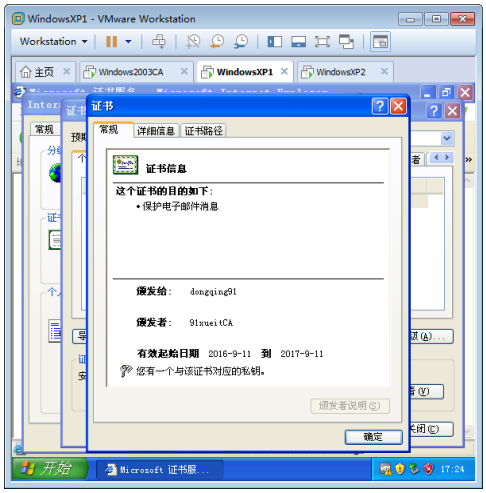

图 10-39　查看用户证书

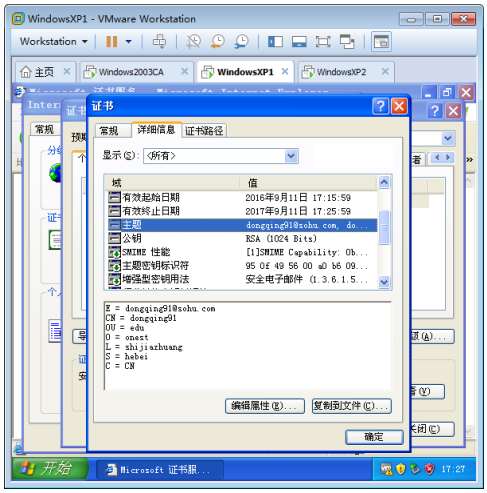

图 10-40　查看使用者信息

如图 10-41 所示，在“详细信息”选项卡下，点击“公钥”，可以看到该证书的公钥，放心，别人看到公钥也没办法算出你的私钥。

如图 10-42 所示，在“证书路径”选项卡中可以看到哪个证书颁发机构给谁颁发的证书，选中 91xueitCA，点击“查看证书”，还可以看到该证书颁发机构的信息和公钥。

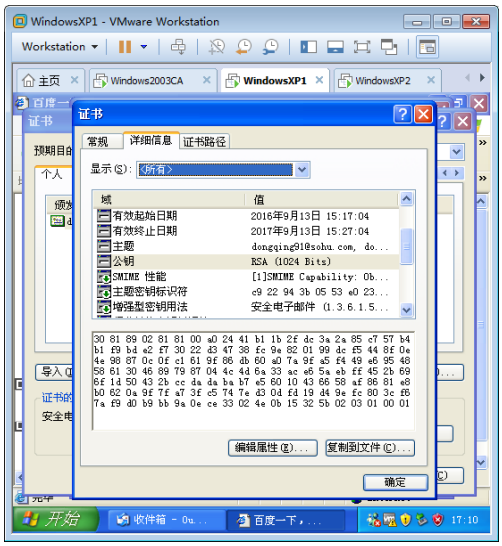

图 10-41　查看证书公钥

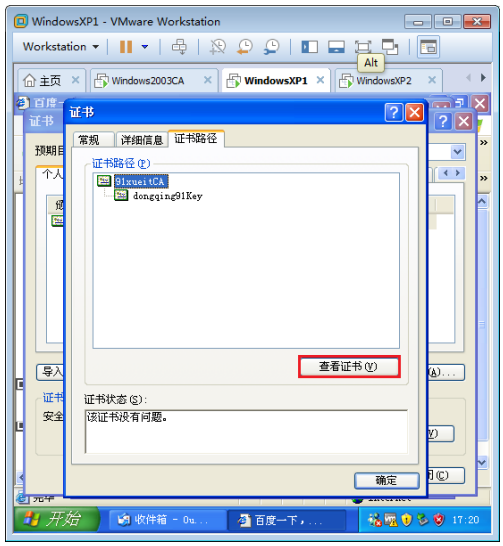

图 10-42　查看证书颁发机构

如图 10-43 所示，在“证书”对话框的“个人”选项卡下，选中申请的证书，点击“导出”。导出证书就是备份数字证书，可以将其导入到其他计算机。

如图 10-44 所示，在出现的“导出私钥”对话框中选择“是，导出私钥”，点击“下一步”。

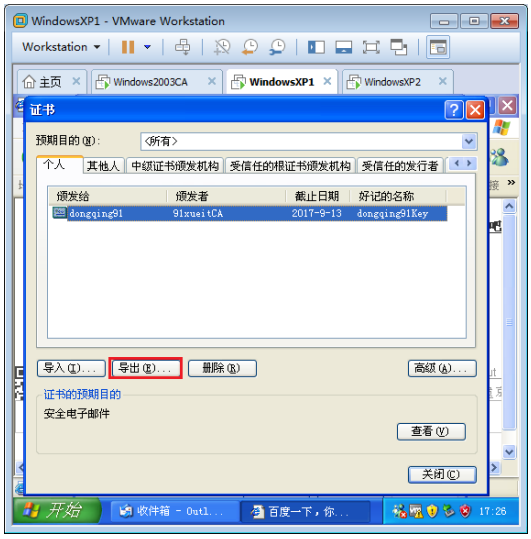

图 10-43　导出证书

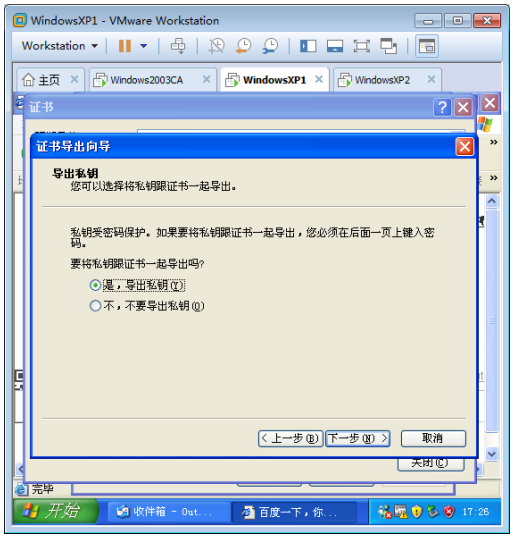

图 10-44　导出私钥和公钥

如果我们选择“不，不要导出私钥”，则导出的证书不包含用户私钥，只有用户公钥，只包含用户公钥的证书可以通过任何途径发送给其他人。

如图 10-45 所示，在出现的“导出文件格式”对话框中保持默认选项，点击“下一步”。

如图 10-46 所示，在出现的“密码”对话框中指定密码，点击“下一步”，以后导入证书时就需要输入该密码。

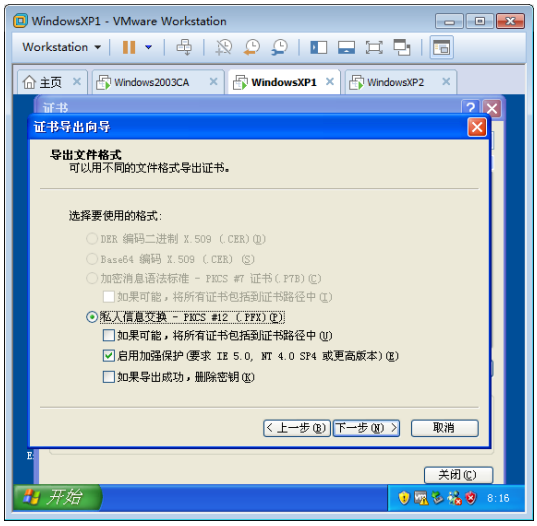

图 10-45　指定导出的格式

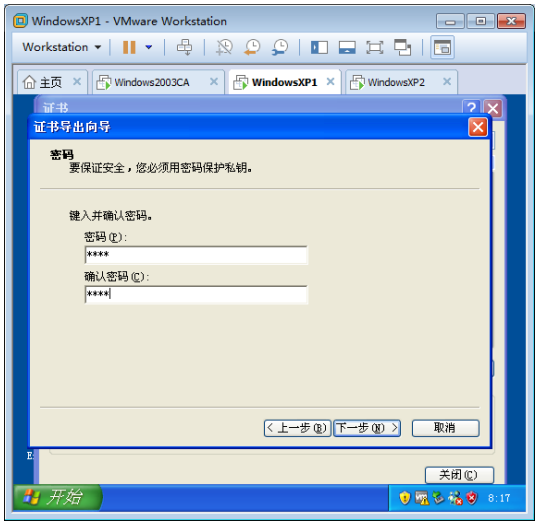

图 10-46　设置密码

如图 10-47 所示，在出现的“要导出的文件”对话框中指定文件路径和名称，点击“下一步”。

如图 10-48 所示，在出现的“正在完成证书导出向导”对话框中点击“完成”。

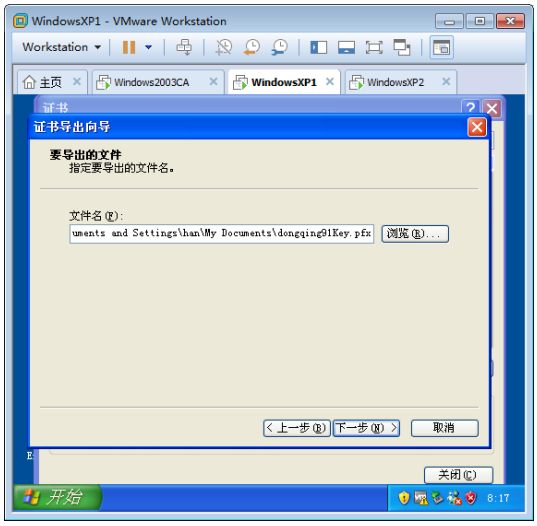

图 10-47　指定导出的文件

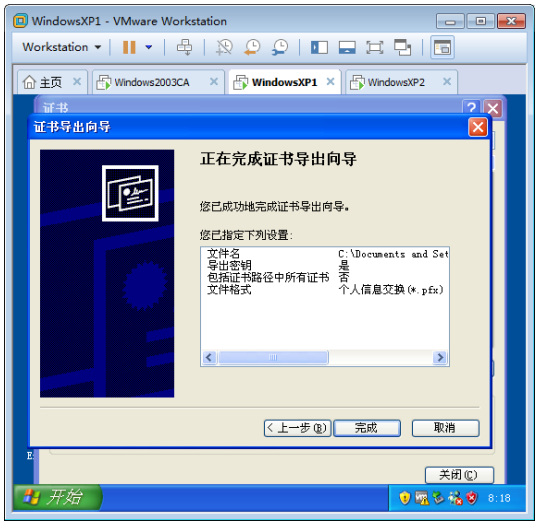

图 10-48　完成导出

10.3.3　配置 Outlook Express 账户绑定数字证书

在 WindowsXP1 上配置 Outlook Express 使用的电子邮件账户和收发电子邮件的服务器以及使用的协议。

如图 10-49 所示，打开 Outlook Express，在出现的“您的姓名”对话框中输入显示名，点击“下一步”。

如图 10-50 所示，在出现的“Internet 电子邮件地址”对话框中输入电子邮件地址，点击“下一步”。

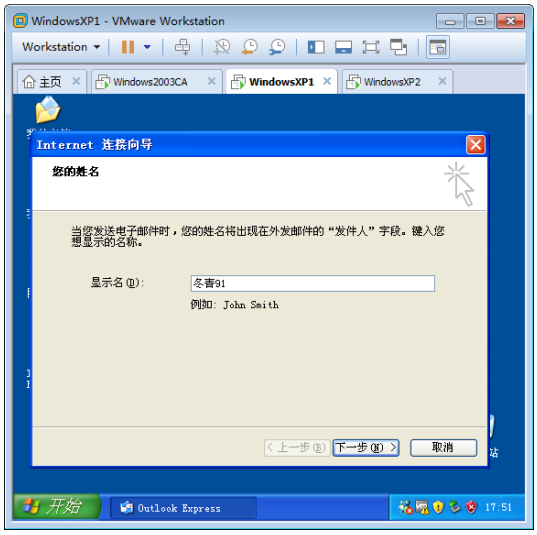

图 10-49　输入显示名

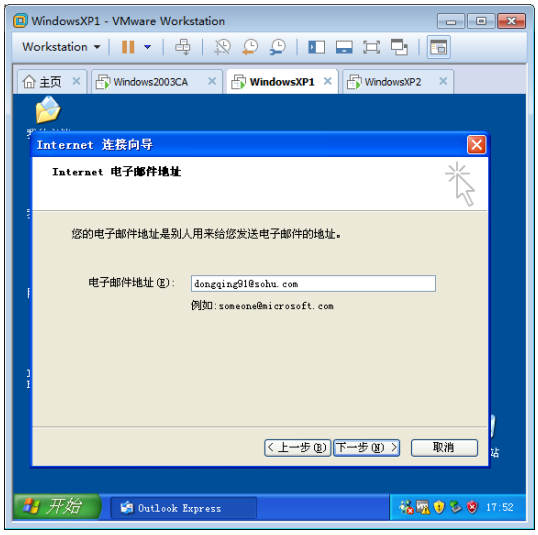

图 10-50　输入电子邮件地址

如图 10-51 所示，在出现的“电子邮件服务器名”对话框中选择使用的接收邮件的协议为 POP3，指定接收邮件的服务器和发送邮件的服务器，点击“下一步”。

如图 10-52 所示，在出现的“Internet Mail 登录”对话框中输入账户名和密码，选中“记住密码”，点击“下一步”，完成 Internet 连接向导的设置。

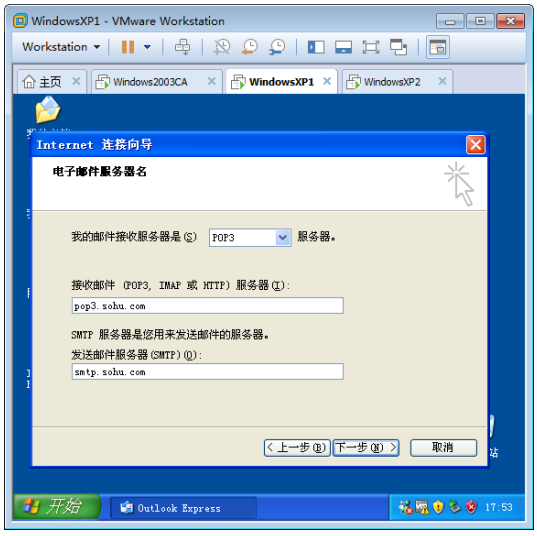

图 10-51　设置接收和发送邮件服务器

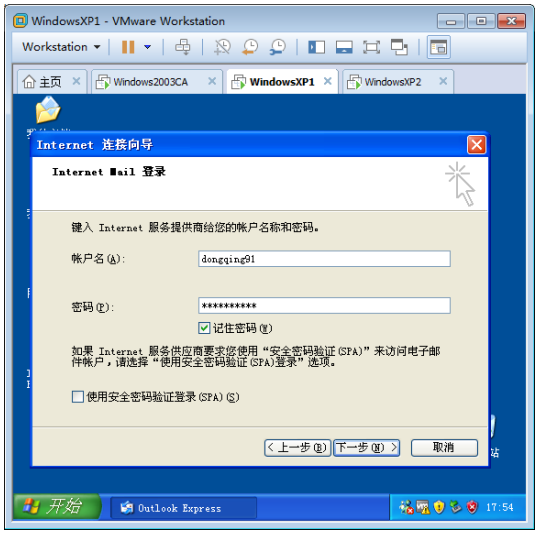

图 10-52　输入用户名和密码

如图 10-53 所示，点击 Outlook Express“工具”菜单，点击“账户”。

如图 10-54 所示，在出现的“Internet 账户”对话框的“邮件”选项卡下，选中 pop3.sohu.com，点击“属性”。

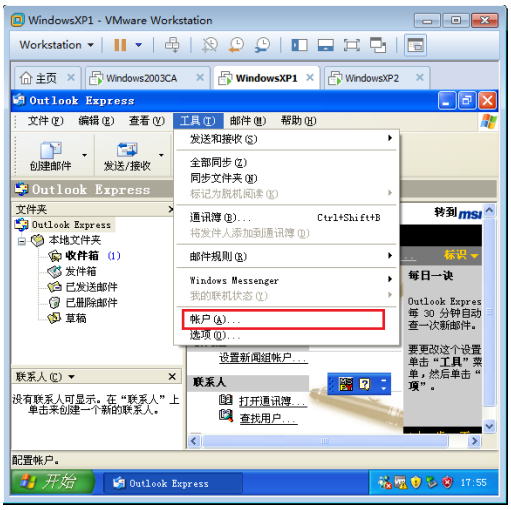

图 10-53　设置账户属性

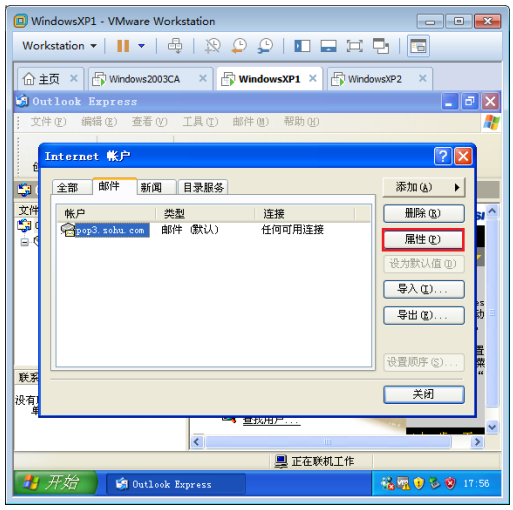

图 10-54　打开账户属性

如图 10-55 所示，在出现的“pop3.sohu.com 属性”对话框的“服务器”选项卡下，选中“我的服务器要求身份验证”，默认不允许匿名中继，所以要选择该项。

如图 10-56 所示，在“安全”选项卡下，签署证书中点击“选择”，选中用于数字签名的证书。

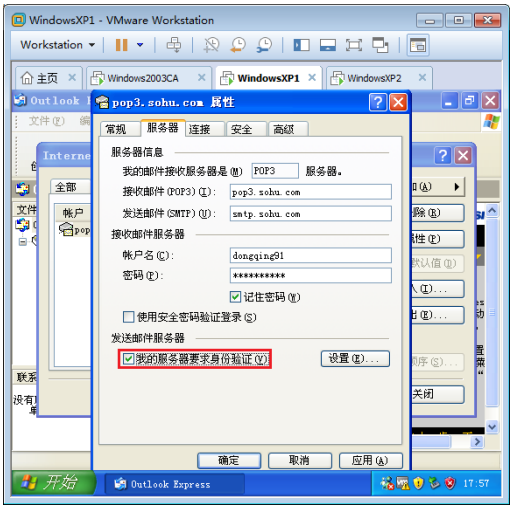

图 10-55　设置发送身份

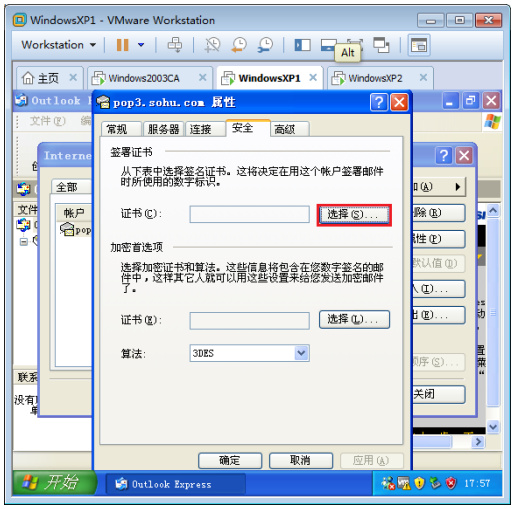

图 10-56　选择数字证书

如图 10-57 所示，在出现的“选择默认账户数字 ID”对话框中选择证书，点击“确定”。

如果在这里看不到你申请的数字证书，要检查当时申请数字证书时填写的电子邮件地址和 Outlook Express 中配置的电子邮件地址是否一样，还要检查证书类型是否选择的“电子邮件保护证书”，如果有错误，要重新申请证书。

如图 10-58 所示，在加密首选项中也选择这个证书。因为用户发送签名的邮件时会把用户公钥

一起给接收者，接收者就可以使用这个公钥发送加密邮件。在这里还可以指定算法，点击“应用”，关闭“pop3.sohu.com 属性”对话框。

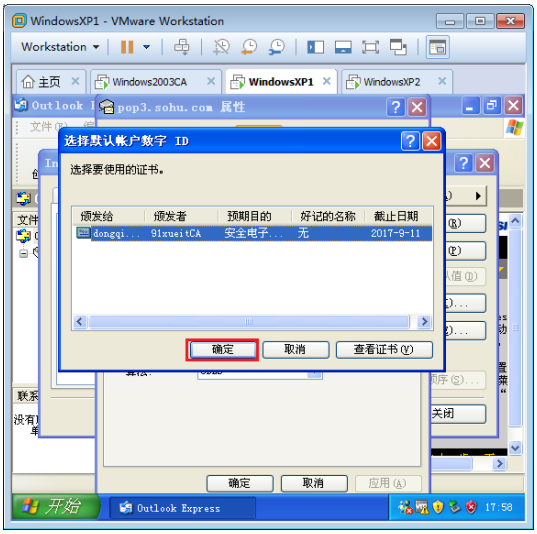

图 10-57　选择签名数字证书

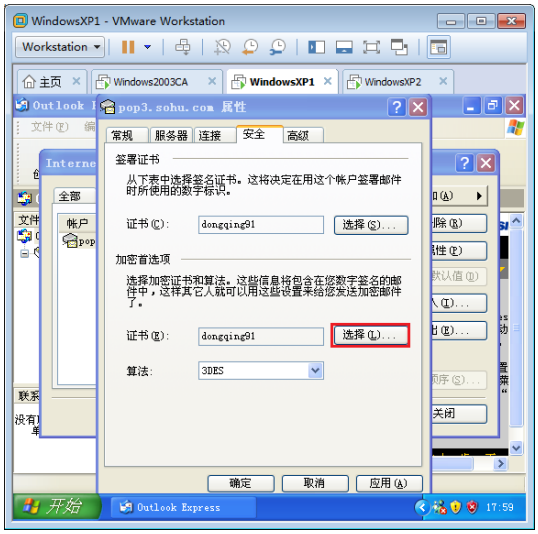

图 10-58　选择加密数字证书

10.3.4　发送数字签名的邮件

用户有了数字证书，就可以给别人发送数字签名的邮件了。下面来给 dongqing081@sohu.com 发送一封数字签名的邮件。

如图 10-59 所示，写一封电子邮件，点击“签名”，再点击“发送”。

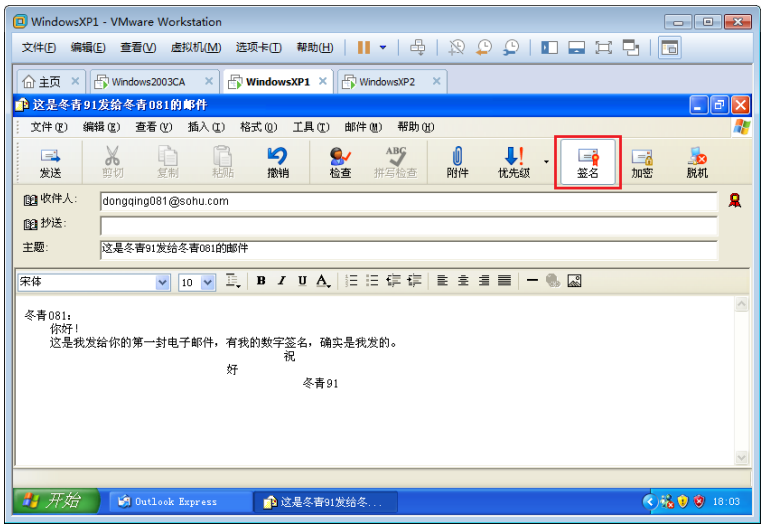

图 10-59　发送签名电子邮件

在这里不能点击“加密”，因为加密需要收件人的公钥，现在还没有这个收件人的公钥，所以不能点击“加密”。

在 WindowsXP2 上，配置 Outlook Express 使用 dongqing081@sohu.com 电子邮箱。如图 10-60 所示，接收电子邮件，可以看到收到一份数字签名的电子邮件，有标记，点击“继续”。

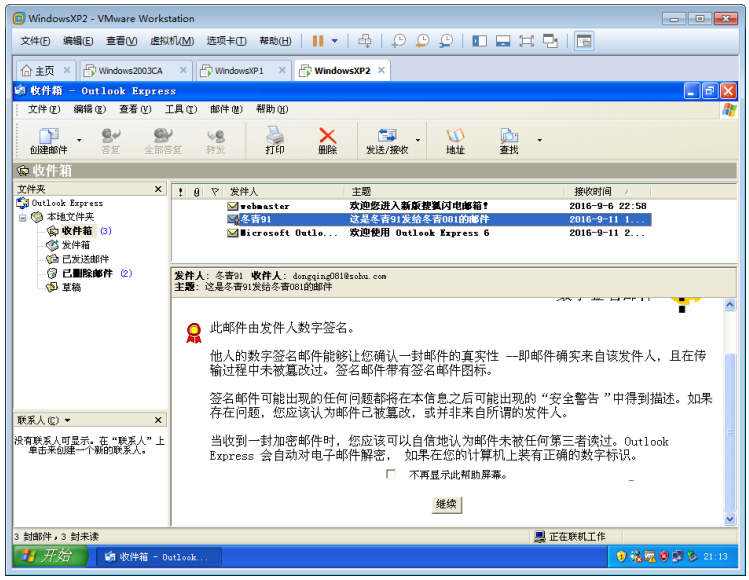

图 10-60　打开数字签名的邮件

如图 10-61 所示，出现安全警告，为什么呢？大家思考一下，自己安装的证书颁发机构，WindowsXP2 上的用户信任么？不信任。所以出现安全警告“目前您还未做出决定是否使用该数字标识签发这封邮件”。参照 10.3.2 节的操作信任该证书颁发机构。

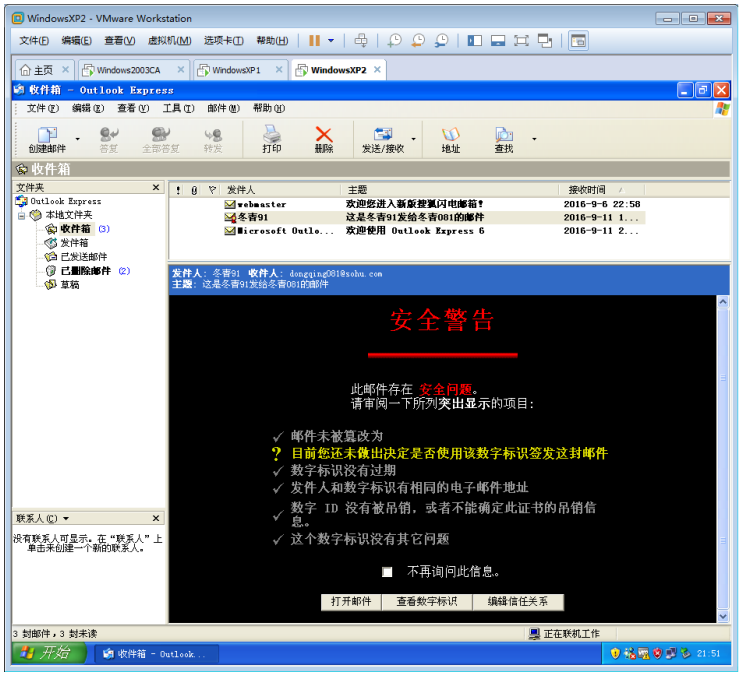

图 10-61　不信任证书颁发机构

Outlook Express 会自动检查数字签名是否有效，如果邮件被篡改，签名的数字证书过期，证书颁发机构不受信任，发件人和数字证书标识的电子邮件不相同都会出现安全警告。数字签名和验证数字签名都需要应用程序来完成，对用户来说是透明的。

再次打开该邮件，如图 10-62 所示，就不再出现安全警告，大家留意该邮件有数字签名标记，同时还自动创建了一个联系人。

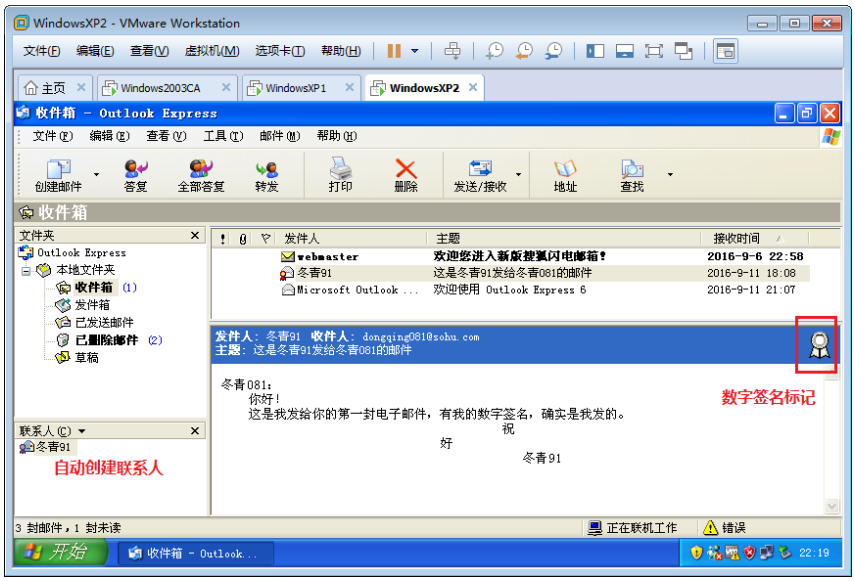

图 10-62　收到数字签名的邮件会自动创建联系人

10.3.5　发送加密的邮件

dongqing91@sohu.com 给 dongqing081 发送了一封数字签名的电子邮件。这封电子邮件就带有 dongqing91@sohu.com 的公钥，所以 Outlook Express 自动创建了一个联系人，该联系人和他的公钥绑定。

如图 10-63 所示，右击“冬青 91”，点击“属性”。在出现的“冬青 91 属性”对话框的“数字标识”选项卡下，可以看到该联系人的电子邮件地址和该电子邮件地址相关联的数字表示，也就是数字证书。点击“属性”，就能看到该数字证书，该数字证书有冬青 91 的公钥，可以给他发送一封加密的邮件。

双击“冬青 91”联系人，如图 10-64 所示，出现写电子邮件的界面，写一封电子邮件，点击“加密”按钮，再点击“发送”，出现安全警告，说您没有数字标识，无法在已发送邮件文件夹中阅读这封邮件，点击“是”。

大家思考，在这里能不能把签名也选中？不能，为什么？因为该用户没有自己的数字证书，也就是说他没有私钥，所以不能发送签名的电子邮件，如果他也申请了一个电子邮件证书，他就可以发送签名和加密的电子邮件了。签名使用自己的私钥，加密使用收件人的公钥。先进行签名，再对签名的全部内容进行加密。

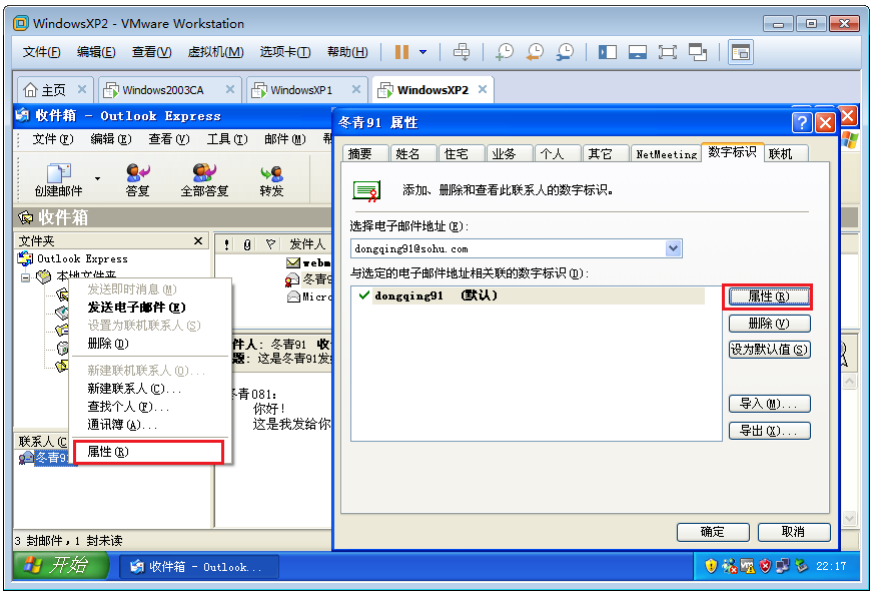

图 10-63　联系人和数字证书（公钥）关联

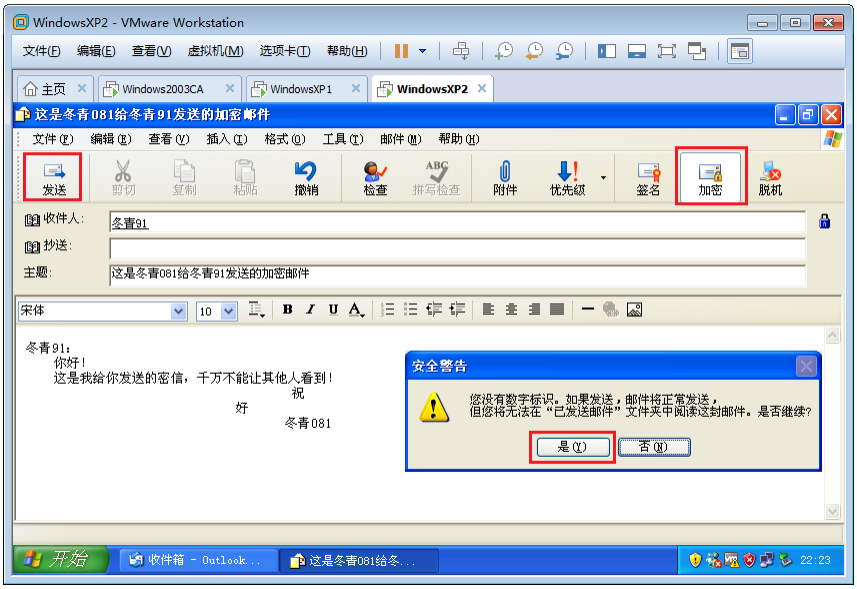

图 10-64　发送加密的电子邮件

在 WindowsXP1 上，如图 10-65 所示，打开 Outlook Express，点击“发送和接收”，选中“收件箱”，可以看到收到的加密邮件，有标记，提示此邮件由发件人加密，未被其他人读过，点击“继续”。

如图 10-66 所示，就可以看到邮件的内容，私钥解密过程对用户来说是透明的，是 Outlook Express 实现的。如果当前用户没有私钥，就不能解密该电子邮件，读取其中的内容了。

现在来演示没有私钥不能解密公钥加密的邮件的情况。

如图 10-67 所示，打开“Internet 选项”对话框，打开“证书”对话框，在“个人”选项卡下，

选中用户的数字证书，点击“删除”，出现提示对话框，提示“不能解密用证书加密的数据，要删除证书吗？”，点击“是”。

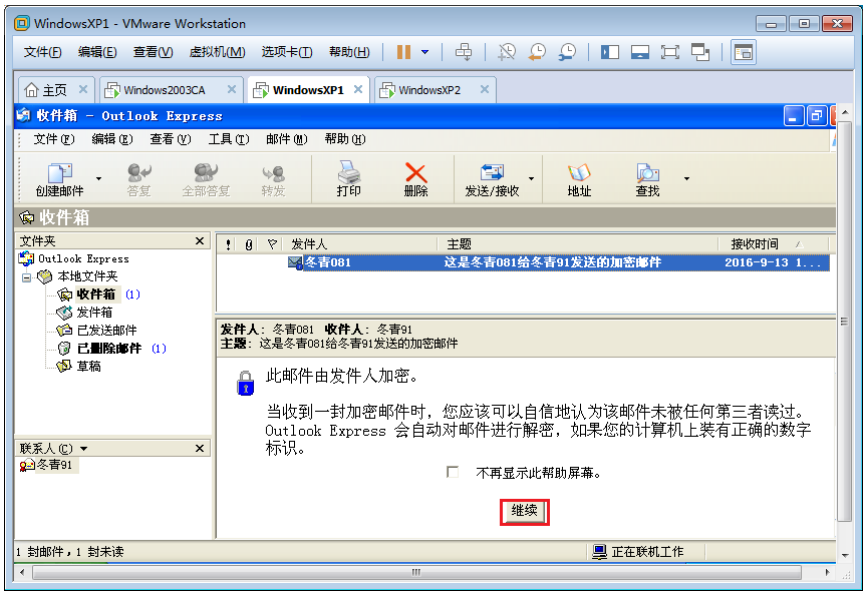

图 10-65　接收到加密的电子邮件

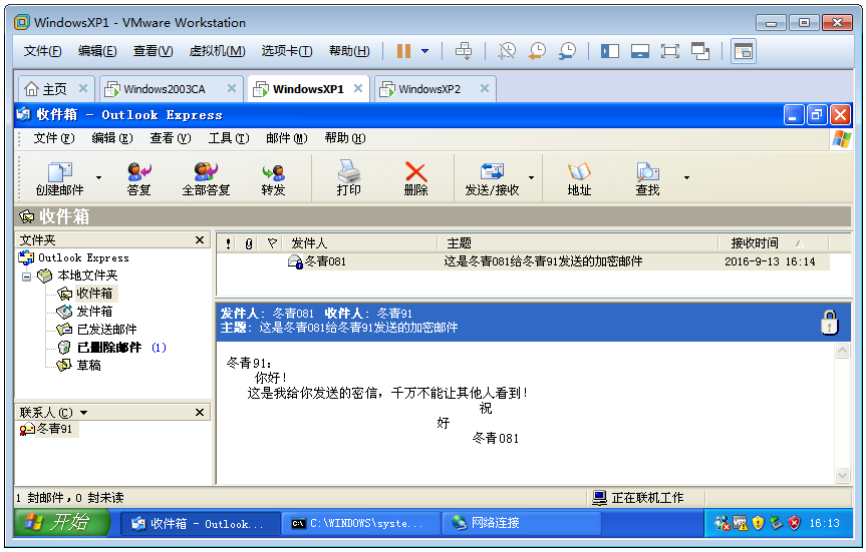

图 10-66　能够解密查看邮件内容

如图 10-68 所示，再次点击 Outlook Express 收件箱，选中收到的加密邮件，不能看到邮件的内容和标题，出现“对邮件加密时出错”，其实是解密时出错。

现在验证，只要导入数字证书，就能解密加密的邮件。

再次打开“Internet 选项”对话框，打开“证书”对话框，在“个人”选项卡下，点击“导入”。浏览到当时导出证书的路径，如图 10-69 所示，看不到当时导出的证书，文件类型选择“所有文件”，就会看到导出的证书，选中该数字证书，点击“打开”。

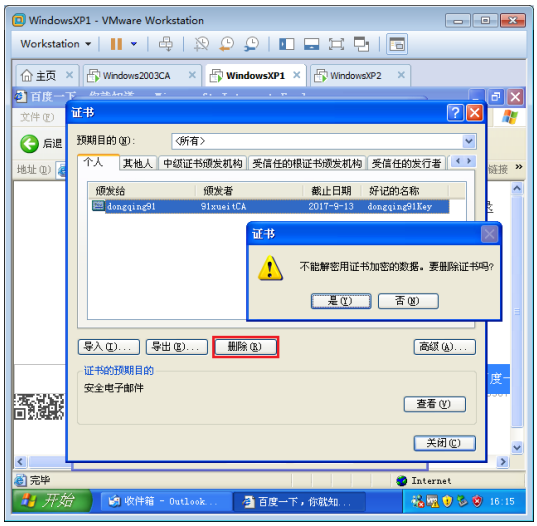

图 10-67　删除用户数字证书

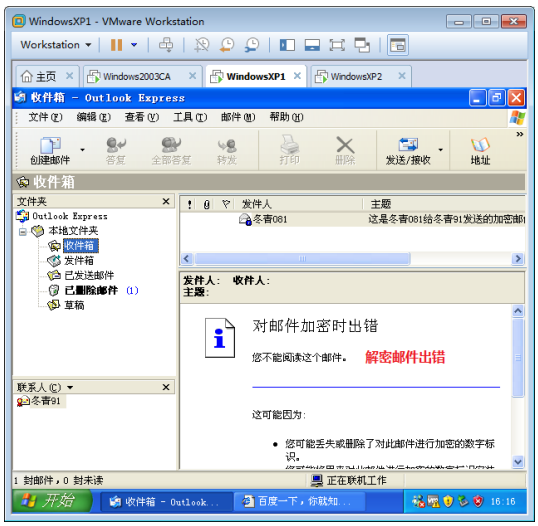

图 10-68　不能解密电子邮件

如图 10-70 所示，证书导入向导出现输入密码对话框，输入当时导出时设置的密码，点击“下一步”。

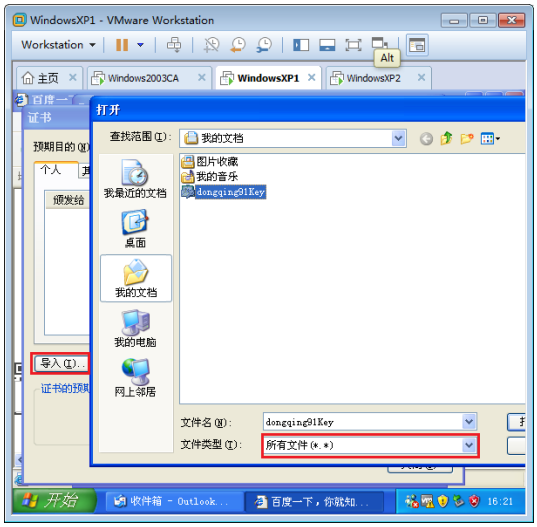

图 10-69　导入电子邮件

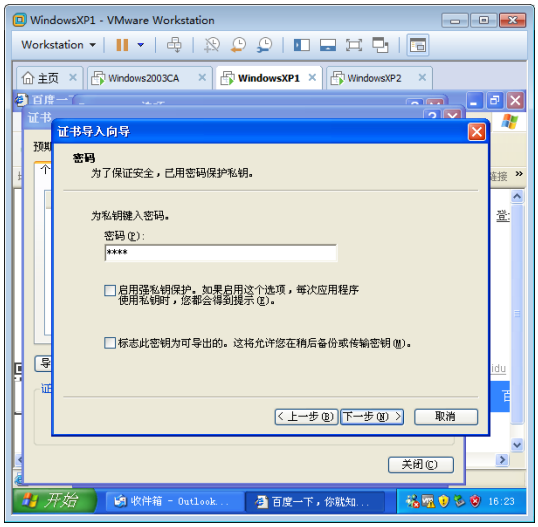

图 10-70　输入密码

> 设置这个密码其实就是对数字证书的保护，即便有人窃取了你的数字证书，但不知道导入密码，也没有办法使用。

导入数字证书后，再次打开收件箱的加密邮件，就能解密加密的电子邮件了。可见，只要导出数字证书，即便改变了计算机或重装了系统，只要导入数字证书就可以解密。

通过上面的学习，我们学会了安装证书颁发机构，申请电子邮件证书，发送签名和加密电子邮件。其实我们开通网银时，银行给我们的 U 盾就是个客户端数字证书。目前数字签名、数字加密已经在网络中得到了广泛应用。

10.4 安全套接字层

TCP/IP 协议本来是四层：应用层、传输层、网络层、网络接口层。这四层，没有一层是专门负责通信安全的。

当万维网能够提供网上购物时，安全问题马上就被提到桌面上，例如用户通过浏览器进行网上购物时，需要以下一些安全措施：

（1）顾客需要确保所浏览的服务器属于真正的厂商而不是假冒的厂商。因为顾客不愿意把他的信用卡号交给一个冒充者。换言之，服务器必须被鉴别。在有些应用中服务器还需要验证顾客身份，比如是否是 VIP 会员。

（2）顾客与销售商需要确保购物报文在传输过程中没有被篡改。比如 100 元的账单一定不能被篡改为 1000 元的账单。

（3）顾客与销售商需要确保诸如信用卡、登录网址的账户和密码等敏感信息不被因特网的入侵者截获，这就需要对购物的报文进行加密。

使用 http 协议访问网站存在以下风险：

（1）窃听风险（eavesdropping）：第三方可以获知通信内容。

（2）篡改风险（tampering）：第三方可以修改通信内容。

（3）冒充风险（pretending）：第三方可以冒充他人身份参与通信。

为了避免以上风险，在应用层和传输层之间增加了一层——安全套接字层，来解决上述安全问题。如图 10-71 所示，安全套接字层广泛使用的有两个协议 SSL 和 TLS。

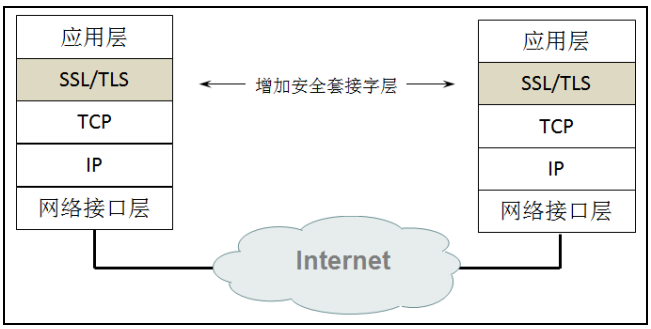

图 10-71　新增安全套接字层

SSL/TLS 协议是为了解决上述三大风险而设计的，希望达到：

（1）所有信息都是加密传播，第三方无法窃听。

（2）具有校验机制，一旦被篡改，通信双方会立刻发现。

（3）配备身份证书，防止身份被冒充。

10.4.1 安全套接字层（SSL）和传输层安全（TLS）

安全套接字层（Secure Socket Layer，SSL）是 Netscape 公司在 1994 年开发的安全协议。SSL 作用在应用层和传输层之间，为访问网站的 http 流量建立一个安全的通道。SSL 最新的版本是 1996

年的 SSL3.0。虽然它还没有成为正式标准，但已经是保护万维网的 HTTP 通信公认的事实上的标准了。

1995 年 Netscape 公司把 SSL 转交给 IETF，希望能够把 SSL 标准化。IETF 将 SSL 作了标准化，即 RFC2246，并将其称为 TLS（Transport Layer Security），其最新版本是 RFC5246 版本 1.2。从技术上讲，TLS1.0 与 SSL3.0 的差异非常微小。

现在很多浏览器都已使用了 SSL 和 TLS，如图 10-72 所示，打开 Windows 7 的 IE 浏览器属性对话框，在“高级”选项卡下可以看到默认已经选中了“使用 SSL2.0”“使用 SSL3.0”“使用 TLS1.0”“使用 TLS1.1”“使用 TLS1.2”。

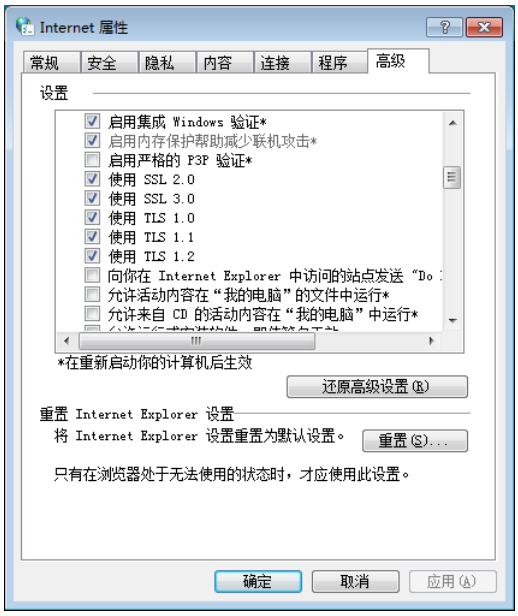

图 10-72　IE 浏览器支持 SSL 版本

安全套接字层应用最多的就是 HTTP，但不局限于 HTTP。当应用层协议使用安全套接字实现安全传输时，就会使用另一个端口，同时给出一个新的名字，即在原协议名字后面添加 S，S 代表 security。比如：

HTTP 协议使用安全套接字层，协议名字就变为 HTTPS，端口为 443。

IMAP 协议使用安全套接字层，协议名称就变为 IMAPS，端口为 993。

POP3 协议使用安全套接字层，协议名称就变为 POP3S，端口为 995。

SMTP 协议使用安全套接字层，协议名称就变为 SMTPS，端口为 465。

SSL 提供的安全服务可归纳为以下三种：

（1）SSL 服务器鉴别，允许用户证实服务器的身份。支持 SSL 的客户端通过验证来自服务器的证书，来鉴别服务器的真实身份，并获取服务器的公钥。

（2）SSL 客户鉴别，允许服务器证实客户的身份。这个信息对服务器是重要的。例如，当银行把有关财务的保密信息发送给客户时，就必须检验接收者的身份。

（3）加密的 SSL 会话，客户和服务器交互的所有数据都在发送方加密，在接收方解密。SSL 还提供了一种检测信息是否被攻击者篡改的机制。

在 Windows 安装完毕，微软公司就已经将互联网上那些知名的证书颁发机构添加到计算机和用户的受信任的根证书颁发机构了，我们的计算机就有了这些根证书颁发机构的公钥了。当服务器出示的证书是这些颁发机构颁发的，就可以使用证书颁发机构的公钥来鉴别网站身份。如图 10-73 所示，在“Internet 属性”对话框中，点击“证书”。如图 10-74 所示，在出现的“证书”对话框的“受信任的根证书颁发机构”选项卡中，可以看到已经信任了互联网上知名的证书颁发机构。

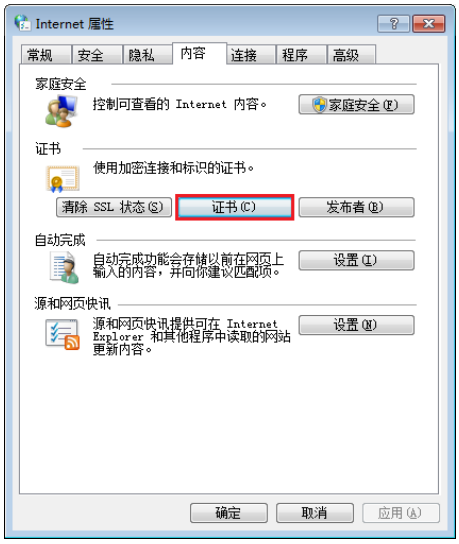

图 10-73　打开用户证书

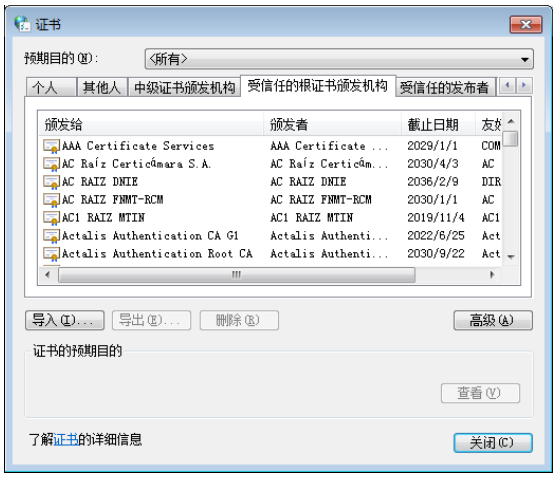

图 10-74　查看用户信任的证书颁发机构

10.4.2　安全套接字层工作过程

要使服务器和客户机使用 SSL 进行安全的通信，服务器必须有服务器证书。证书用来进行身份验证或者身份确认。证书和服务器的域名绑定，这就要求客户端必须使用域名访问服务器，服务

器向客户端出示服务器证书，客户端就要检查访问的域名和证书中的域名是否相同，不同则会出现安全提示。

服务器证书中必须有一对密钥（公钥和私钥），这两个密钥用来对消息进行加密和解密，以确保在因特网上传输时的隐密性和机密性。

证书可以是自签（self-signed）证书，也可以是颁发（issued）证书。自签证书是服务器自己产生的证书，要求客户端信任该证书。如果是证书颁发机构颁发给服务器的证书，客户端必需要信任该证书颁发机构才行。

下面以万维网应用为例来说明 SSL 的工作过程。

现在很多网站当跳转到需要输入敏感信息的页面时，就会使用安全套接字来实现其安全。比如你访问工商银行的网站，在浏览器中输入 http://www.icbc.com.cn，使用 HTTP 协议访问，当你点击“个人网上银行”，会跳转到 https 连接，实现安全通信。建立安全会话的简要过程如图 10-75 所示。

（1）浏览器 A 将自己支持的一套加密算法发送给服务器 B。

（2）服务器 B 从中选出一组加密算法与哈希算法，并将自己的身份信息以证书的形式发回给浏览器。证书里包含了网站域名、加密公钥，以及证书颁发机构等信息。

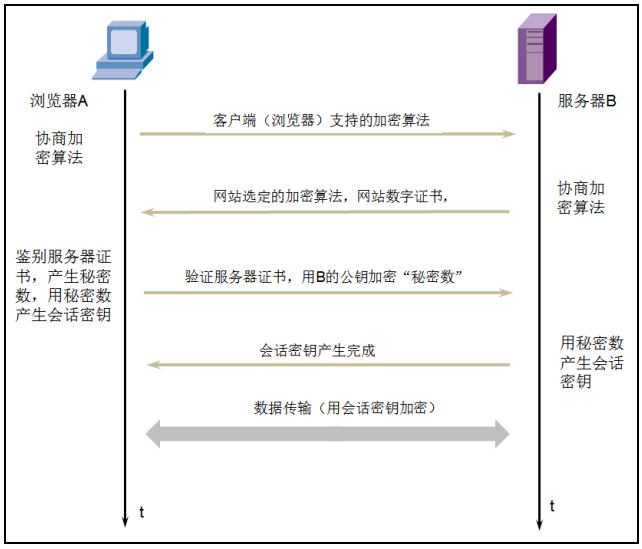

图 10-75　安全套接字建立安全会话的过程

（3）验证证书的合法性（是否信任证书颁发机构，证书中包含的网站域名地址是否与正在访问的地址一致，证书是否过期等），如果证书受信任，浏览器栏里会显示一个小锁头，否则会给出证书不受信任提示。如果证书受信任，或者是用户接受了不受信任的证书，浏览器会产生秘密数，客户端使用秘密数产生会话密钥。秘密数使用服务器 B 提供的公钥加密，发送给服务器。

（4）服务器用私钥解密秘密数，双方根据协商的算法产生会话密钥，这和浏览器 A 产生的会话密钥相同。

（5）安全数据传输。双方用会话密钥加密和解密它们之间传送的数据并验证其完整性。

10.4.3　证书颁发机构层次

CA 认证中心是一个负责发放和管理数字证书的权威机构。认证中心通常采用多层次的分级结

构，如图 10-76 所示，上级认证中心负责签发和管理下级认证中心的证书，最下一级的认证中心直接面向最终用户发放证书。通常情况下，从属 CA 针对特定用途发放证书，例如安全电子邮件、基于 Web 的身份认证或智能卡身份认证。

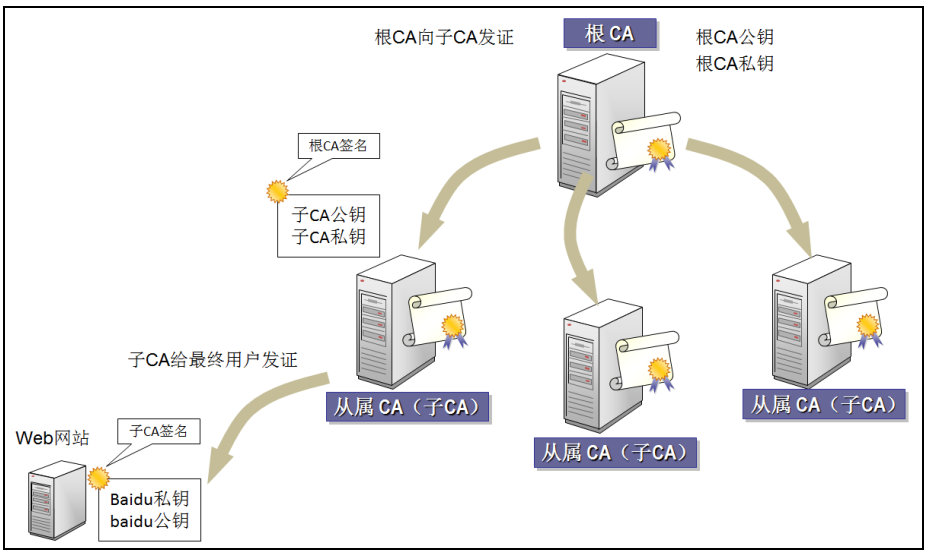

图 10-76　证书的层次结构

层次结构的顶级 CA 称为根 CA，根 CA 的子 CA 称为从属 CA。即证书层次结构的层次包括：根 CA、由根 CA 认证的从属 CA，当然从属 CA 也可以给它的下级 CA 发证。上级 CA 给下级 CA 的数字证书签名。

互联网中的用户只需信任根证书颁发机构，就能信任其所有从属 CA，就能验证所有从属 CA 颁发的用户证书或服务器证书。如图 10-77 所示，百度网站从子 CA 申请了 Web 服务器证书。客户端浏览百度网站，百度网站向客户端出示 Web 证书——子 CA 的证书（只含公钥），在 CA 的证书中有根 CA 的签名。客户端信任根证书颁发机构，就有根证书颁发机构的公钥。

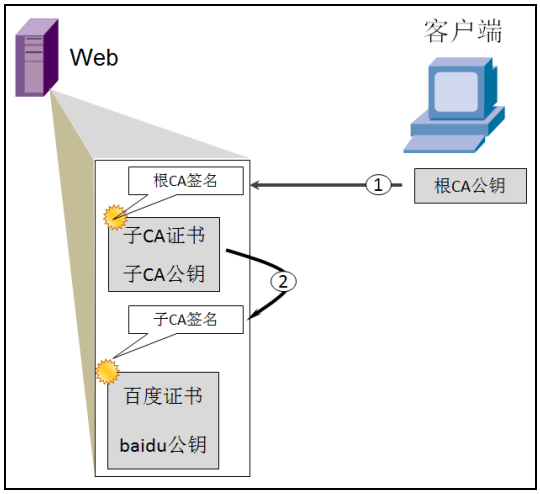

图 10-77　使用根 CA 的公钥验证完整证书的过程

验证过程如下：

（1）客户端先使用根 CA 公钥验证子 CA 的证书，是否是根 CA 颁发的。

（2）验证通过，再使用子 CA 的公钥验证 Web 证书，是否是子 CA 颁发的。

所以说客户端只需要信任根证书颁发机构即可。下面来看看百度网站给用户出示的数字证书。

如图 10-78 所示，访问百度网站查询资料，会自动使用 https 通信，点击网址右侧小锁图标，出现网站标识，点击“查看证书”。

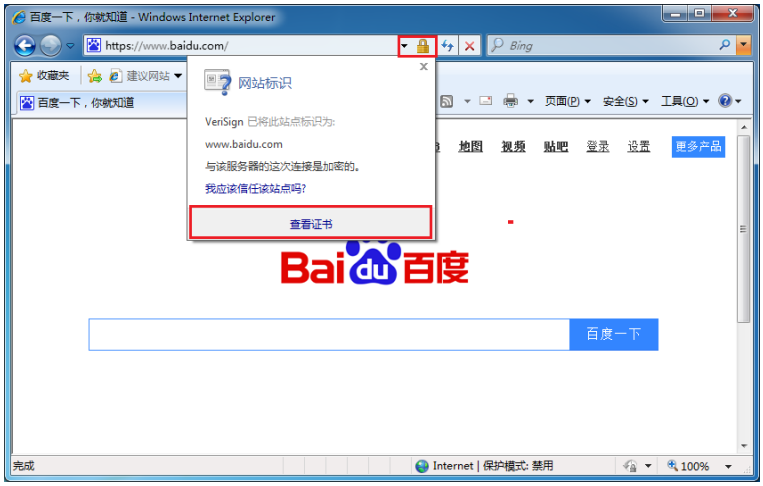

图 10-78　查看网站出示的数字证书

如图 10-79 所示，在出现的“证书”对话框的“常规”选项卡下，可以看到证书的目的、颁发给，颁发者、有效期。

如图 10-80 所示，在“证书路径”选项卡下，可以看到有三级，第一级是 VeriSign，这是根证书颁发机构，第二级是 VeriSign Class 3 Secure CA – G3，是子证书颁发机构，第三级是 baidu.com，是子证书颁发机构给 baidu.com 网站颁发的证书。现在知道证书路径是怎么回事了吧。

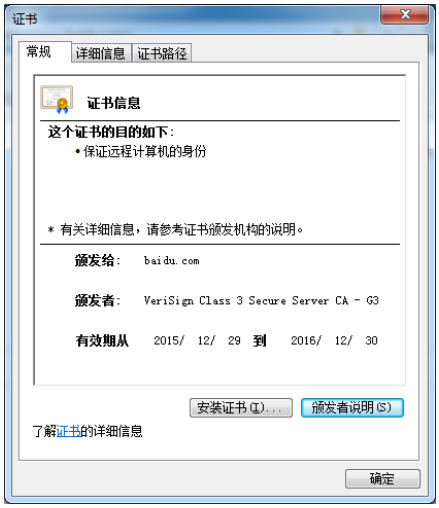

图 10-79　证书信息

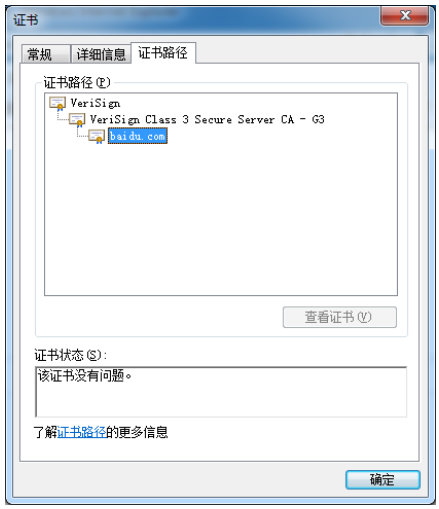

图 10-80　证书路径

10.5 实战：配置网站使用 https 通信

本节演示如何配置 Web 站点使用 https 通信。

以下实验需要三个虚拟机，一个 Windows Server 2003 作为 Web 和 DNS 服务器、一个 Windows Server 2003 作为证书颁发机构（CA），一个 Windows XP 作为浏览器。

10.5.1 申请 Web 服务器证书

Web 站点要想实现 https 通信，必须有 Web 服务器数字证书。注意：这和用户电子邮件数字证书不一样，这个数字证书是计算机证书。

以下操作将会在 Windows2003Web 服务器创建一个 Web 站点，并为该站点申请一个数字证书。

如图 10-81 所示，打开 Internet 信息服务（IIS）管理器，右击“默认网站”，点击“属性”。

如图 10-82 所示，在出现的“默认网站属性”对话框的“目录安全性”选项卡中，点击安全通信下的按钮“服务器证书”。

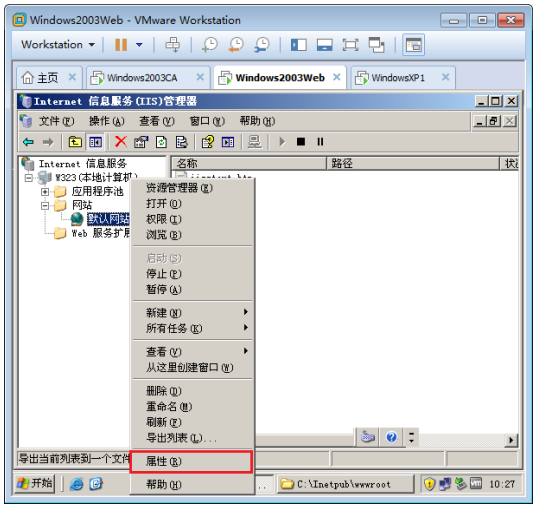

图 10-81 打开网站属性

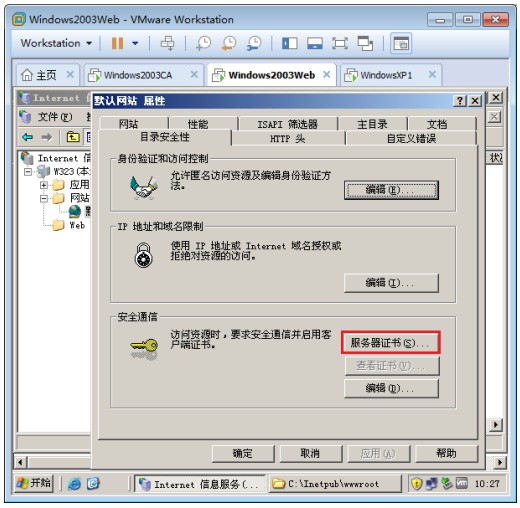

图 10-82 申请服务器证书

如图 10-83 所示，在出现的“服务器证书”对话框中选中“新建证书”，点击“下一步”。

如图 10-84 所示，在出现的“延迟或立即请求”对话框中选中“现在准备证书请求，但稍后发送”，点击“下一步”。这个过程会生成一个证书申请文件。

如图 10-85 所示，在出现的“名称和安全性设置”对话框中输入证书的名称，点击“下一步”。

如图 10-86 所示，在出现的“单位信息”对话框中输入单位信息和部门信息，点击“下一步”。

如图 10-87 所示，在出现的“站点公用名称”对话框中输入用户访问该网站使用的域名，点击“下一步”。

注意：证书的域名和用户访问该网站的域名一定要一样，否则用户在访问该网站时，会出现安全警告。

如图 10-88 所示，在出现的“地理信息”对话框中选择国家，输入省/自治区信息、市县信息，点击“下一步”。

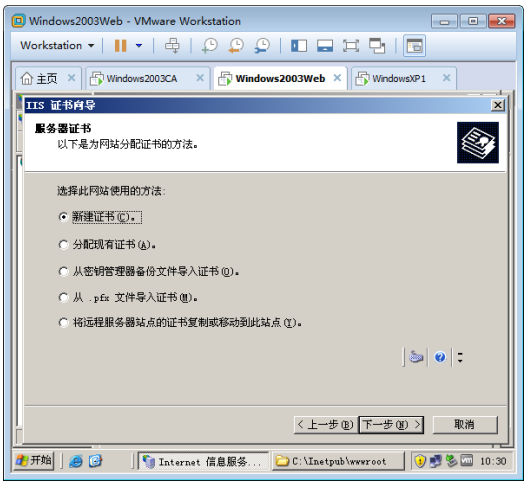

图 10-83　新建证书申请

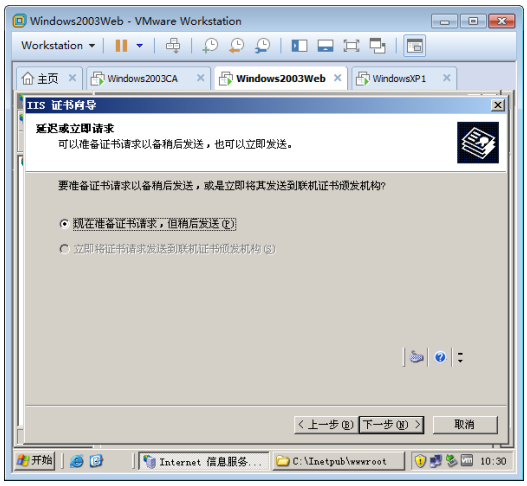

图 10-84　准备证书请求

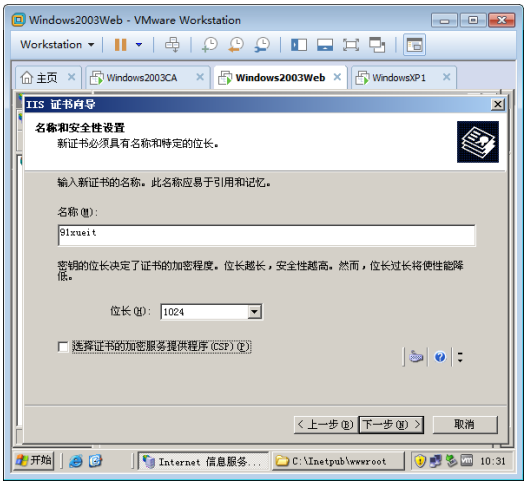

图 10-85　输入证书名称

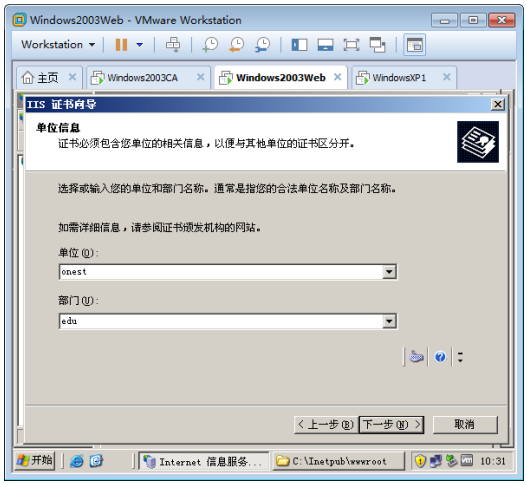

图 10-86　输入单位和部门

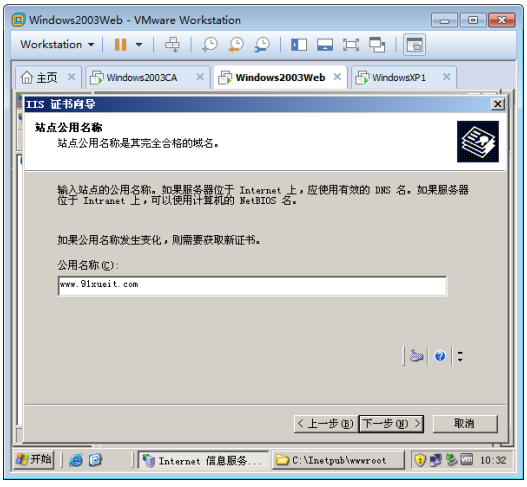

图 10-87　网站域名

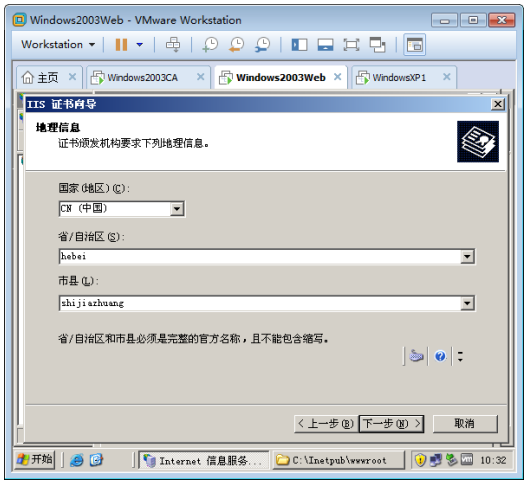

图 10-88　输入地理信息

如图 10-89 所示，在出现的“证书请求文件名”对话框中指定证书请求文件的保存路径和文件名，点击“下一步”。

如图 10-90 所示，在出现的“请求文件摘要”对话框中核实请求包含的信息是否正确，点击“下一步”，完成证书申请文件的准备。

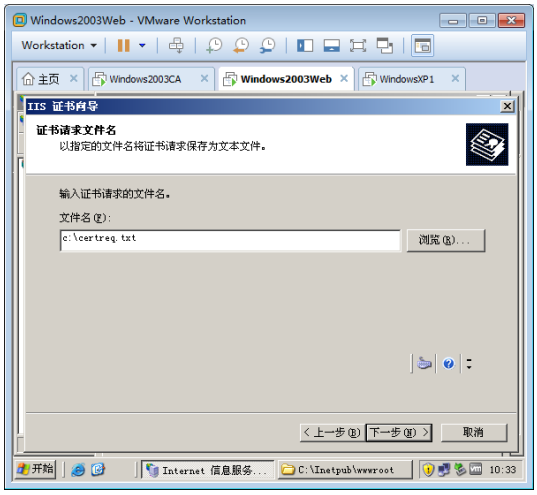

图 10-89　指定保存文件

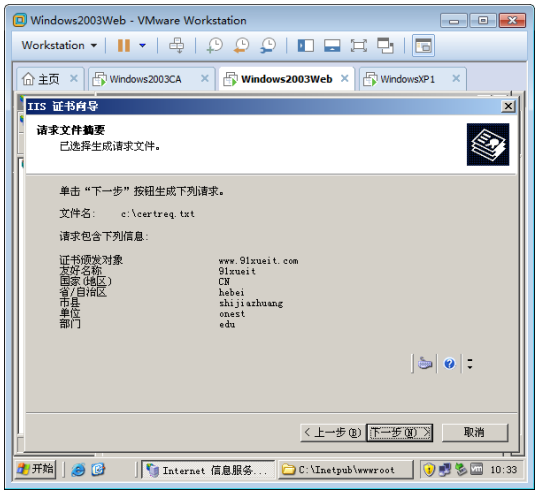

图 10-90　生成证书申请文件

以上是通过向导生成了一个证书申请文件，下面开始申请 Web 服务器证书。

如图 10-91 所示，打开 IE 浏览器，访问证书颁发机构网站，输入 http://192.168.80.10/certsrv，打开首页，点击“申请一个证书”。

如图 10-92 所示，在出现的“申请一个证书”页面点击“高级证书申请”。

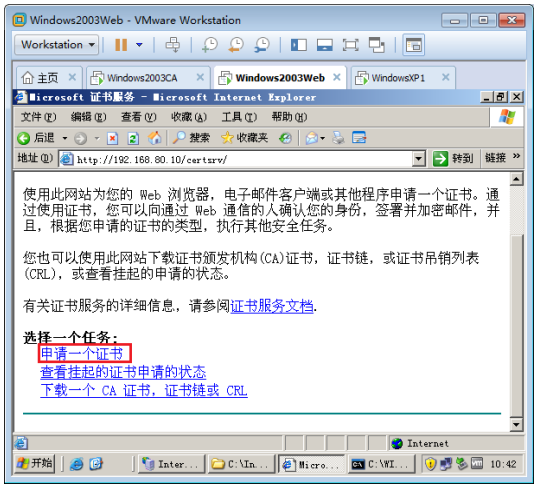

图 10-91　申请证书

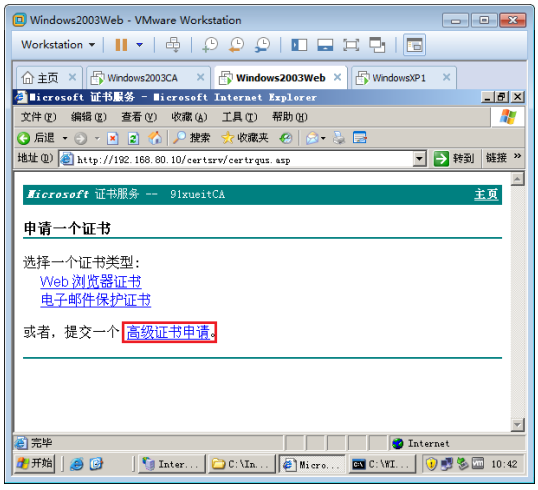

图 10-92　高级申请

如图 10-93 所示，在出现的“高级证书申请”页面点击“使用 base64 编码的 CMC 或 PKCS #10 文件提交一个证书申请，或使用 base64 编码的 PKCS #7 文件续订证书申请”。

如图 10-94 所示，在出现的新页面将生成的证书申请文件的内容复制、粘贴到此处，点击“提交”。

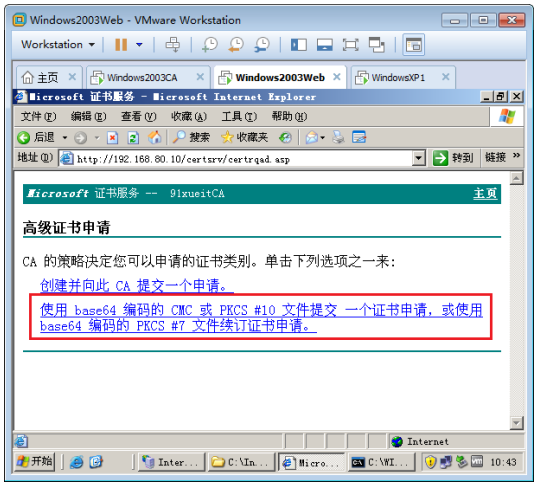

图 10-93　高级申请

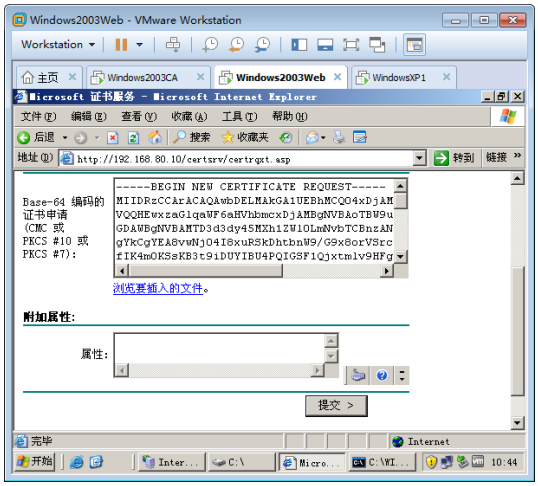

图 10-94　提交申请

如图 10-95 所示，在 Windows2003CA 计算机上，打开证书颁发机构管理工具，选中“挂起的申请”，右击证书，点击“所有任务”→“颁发”。

如图 10-96 所示，在 Web 服务器上打开证书申请首页，点击“查看挂起的证书申请的状态”。

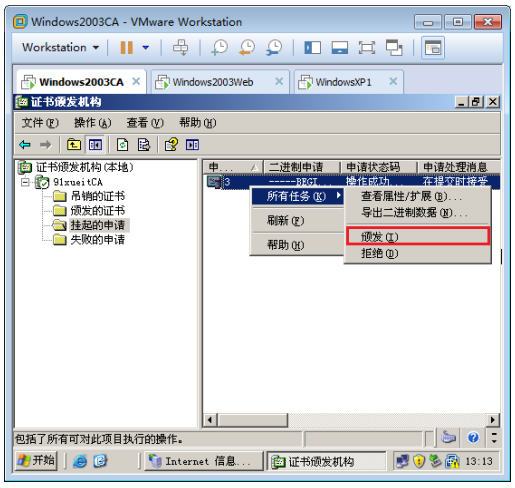

图 10-95　颁发数字证书

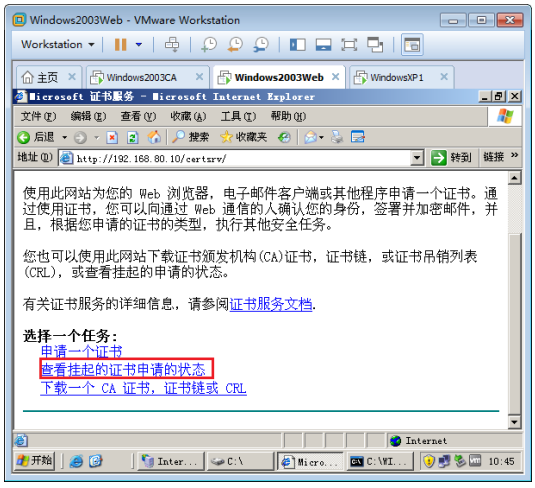

图 10-96　查看挂起的申请

如图 10-97 所示，在出现的“查看挂起的证书申请的状态”页面，点击“保存的申请证书（2016 年 9 月 13 日 10:44:35）”。

如图 10-98 所示，在“证书已颁发”页面选中 DER 编码，点击“下载证书”。指定证书名称，将证书保存到桌面。

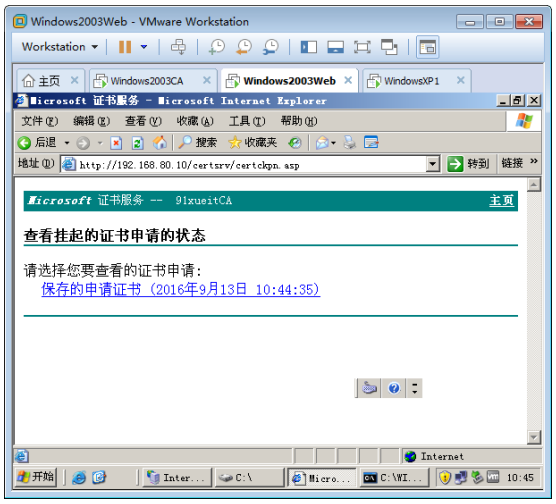

图 10-97　查看证书状态

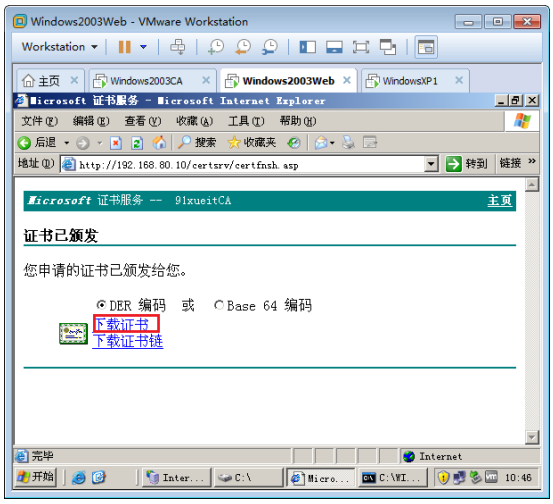

图 10-98　下载证书

10.5.2　配置 Web 站点使用 https 通信

Web 服务器的证书已经保存到桌面，现在需要安装证书，配置网站和该证书进行绑定。

如图 10-99 所示，打开“默认网站属性”对话框，在“目录安全性”选项卡下，点击“服务器证书”。

如图 10-100 所示，在出现的“挂起的证书请求”对话框中选中“处理挂起的请求并安装证书”，点击“下一步”。

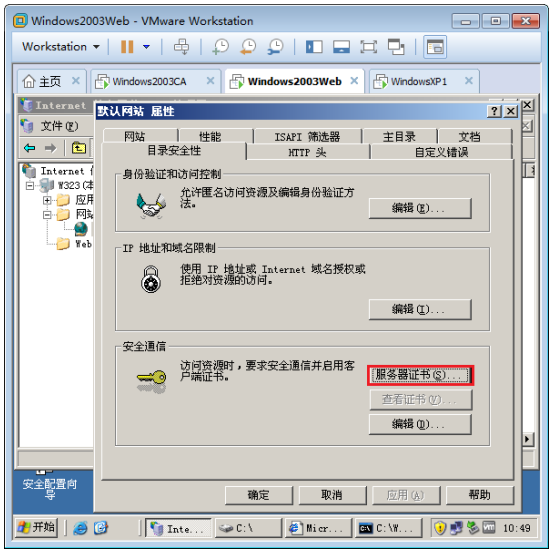

图 10-99　配置 Web 证书

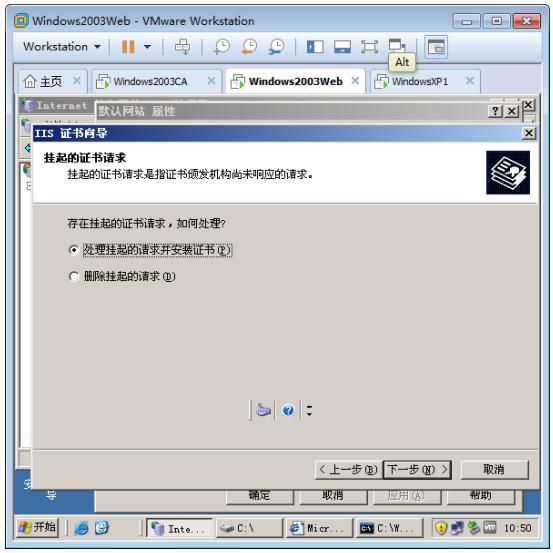

图 10-100　处理挂起的请求

如图 10-101 所示，在出现的“处理挂起的请求”对话框中浏览到保存的证书，点击“下一步”。

如图 10-102 所示，在出现的“SSL 端口”对话框中输入 SSL 使用的端口，默认是 443，点击“下一步”。

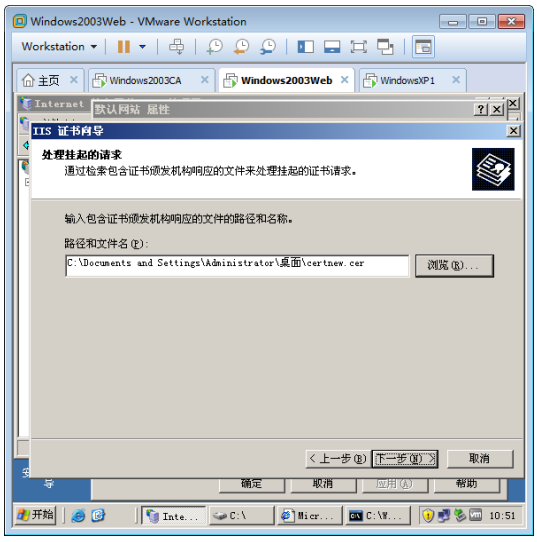

图 10-101　浏览到保存的证书

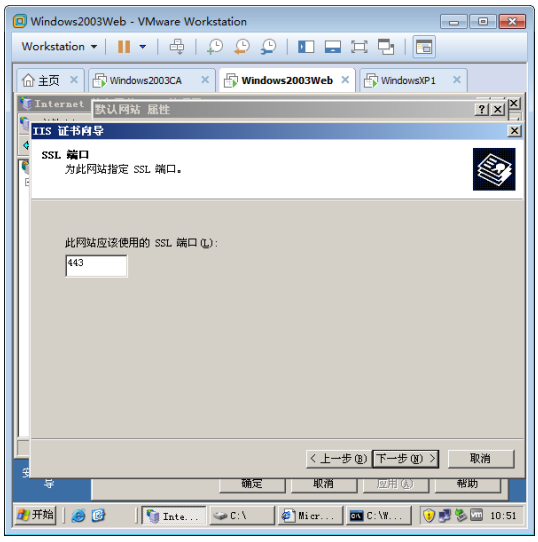

图 10-102　指定 SSL 使用的端口

如图 10-103 所示，在出现的“证书摘要”对话框中点击“下一步”，完成证书向导。

如图 10-104 所示，在“默认网站属性”对话框的“目录安全性”选项卡下，点击“查看证书”。

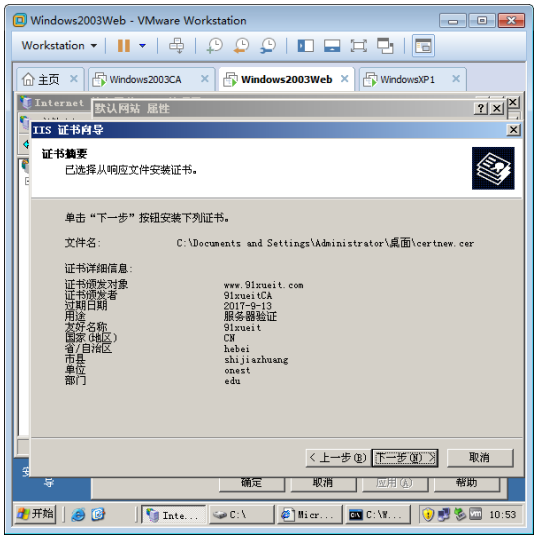

图 10-103　完成证书绑定

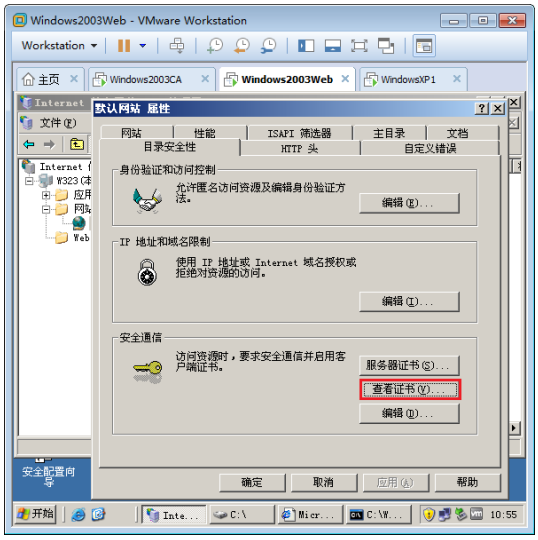

图 10-104　查看网站证书

如图 10-105 所示，在出现的“证书”对话框的“常规”选项卡下，可以看到红色的×，提示不信任颁发这个证书的证书颁发机构。

如图 10-106 所示，在“证书路径”选项卡点击 91xueitCA，点击“查看证书”，可以看到该证书颁发机构的证书（包含公钥）。

如图 10-107 所示，在出现的“证书”对话框的“常规”选项卡下，点击“安装证书”。

如图 10-108 所示，在出现的“证书存储”对话框中选择“将所有的证书放入下列存储”，点击“浏览”。

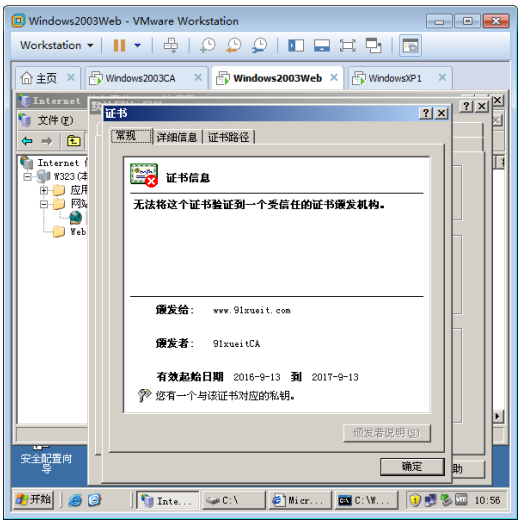

图 10-105　证书颁发机构不受信任

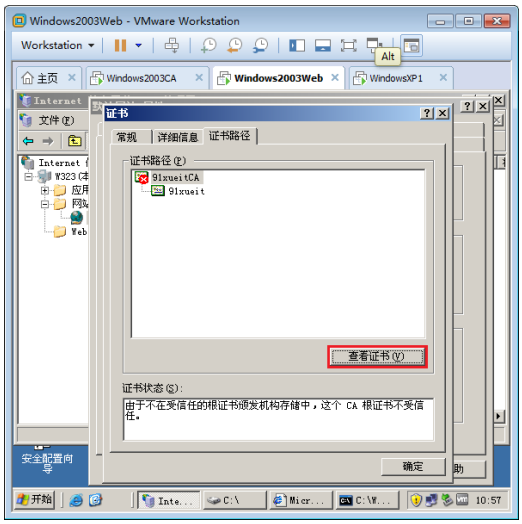

图 10-106　查看证书颁发机构证书（公钥）

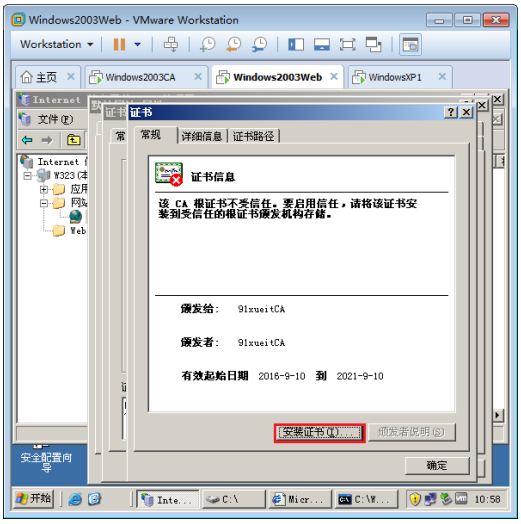

图 10-107　安装根 CA 证书

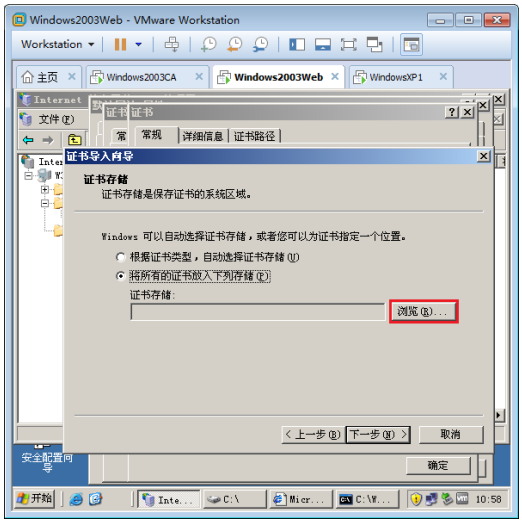

图 10-108　指定证书存储位置

如图 10-109 所示，在出现的“选择证书存储”对话框中勾选“显示物理存储区”，展开受信任的证书颁发机构，选择“本地计算机”，点击“确定”，完成证书的导入。

> 证书分计算机证书和用户证书，当然受信任的证书颁发机构也分计算机信任还是用户信任，注册表示用户信任，本地计算机是计算机信任。

如图 10-110 所示，再次打开“默认网站属性”对话框，在“网站”选项卡下，可以看到 SSL 端口为 443。

如图 10-111 所示，在“目录安全性”选项卡下点击“编辑”。

如图 10-112 所示，在出现的“安全通信”对话框中勾选“要求安全通道（SSL）”和“忽略客户端证书”，点击“确定”，这样就只允许使用 https 协议访问了。如果勾选了“接受客户端证书”，访问该网站必须出示客户端证书。

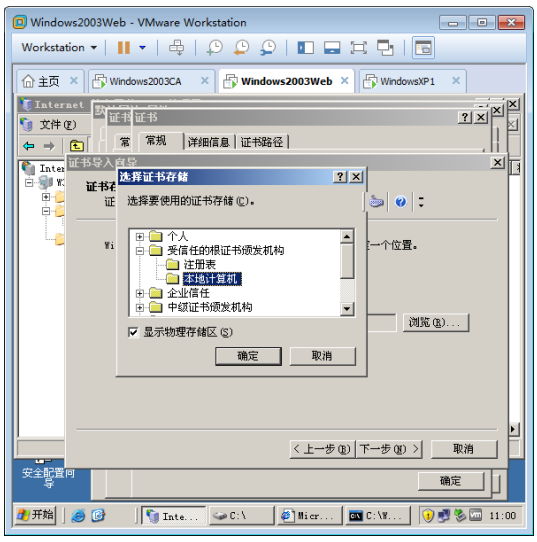

图 10-109　存储在本地计算机

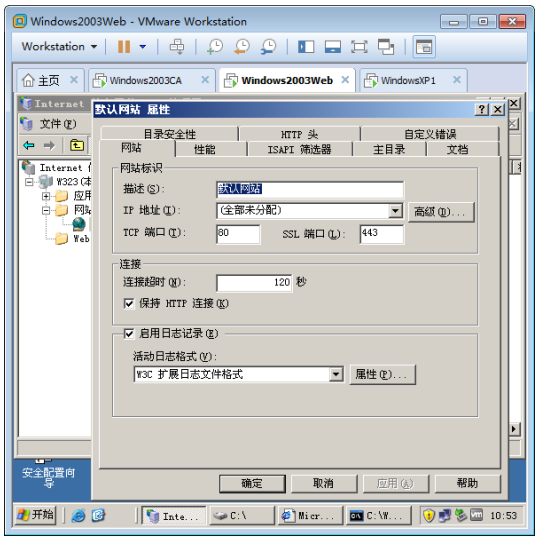

图 10-110　查看 SSL 端口

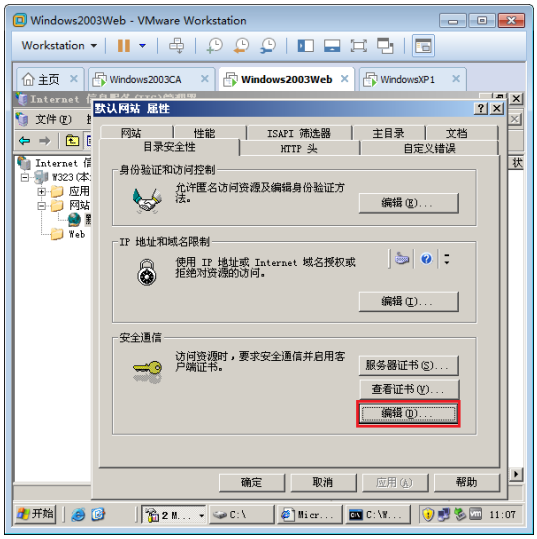

图 10-111　设置安全通信

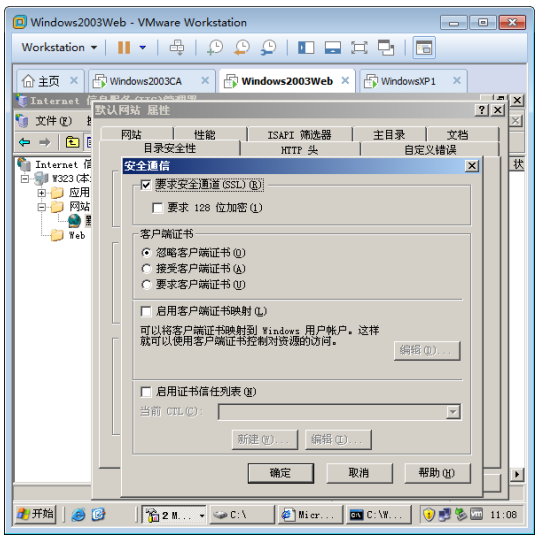

图 10-112　要求安全通信

10.5.3　使用 https 访问网站

给网站申请配置了数字证书，下面在 WindowsXP 测试一下使用 http 和 https 访问该网站。网站绑定了数字证书，数字证书绑定了域名，用户使用数字证书中的域名访问该网站才不会出现安全提示。这就要求 WindowsXP 能够将 www.91xueit.com 解析到 Web 服务器，

在 Web 服务器安装 DNS 服务器，如图 10-113 所示，在正向查找区域创建 91xueit.com，在该区域下创建主机记录 www，IP 地址指向 Web 服务器。

如图 10-114 所示，更改 WindowsXP 使用的 DNS 服务器，确保能将 www.91xueit.com 的域名解析到 Web 服务器的地址。

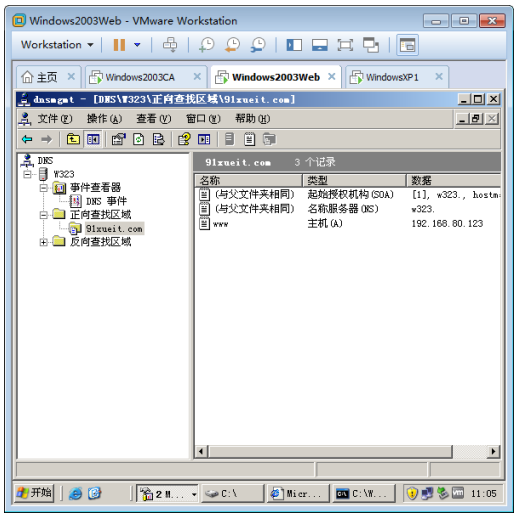

图 10-113　创建 DNS 域和主机记录

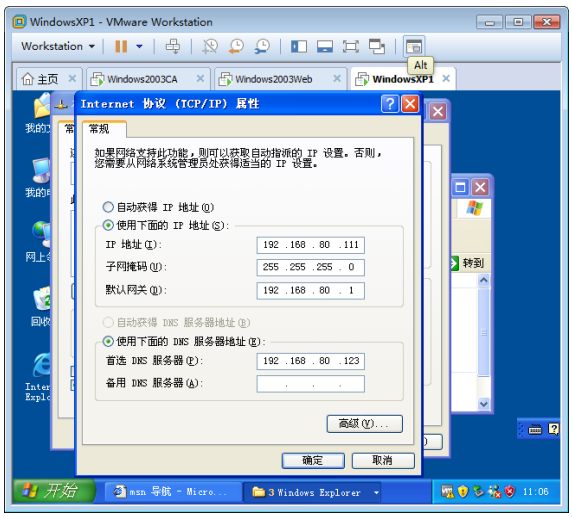

图 10-114　设置使用的 DNS 服务器

如图 10-115 所示，在 WindowsXP 打开 IE 浏览器，输入 http://www.91xueit.com，返回 403.4 错误，提示必须通过安全通道查看。

如图 10-116 所示，在浏览器中输入 https://www.91xueit.com，能够访问成功，在浏览器右下方出现图标，点击图标。

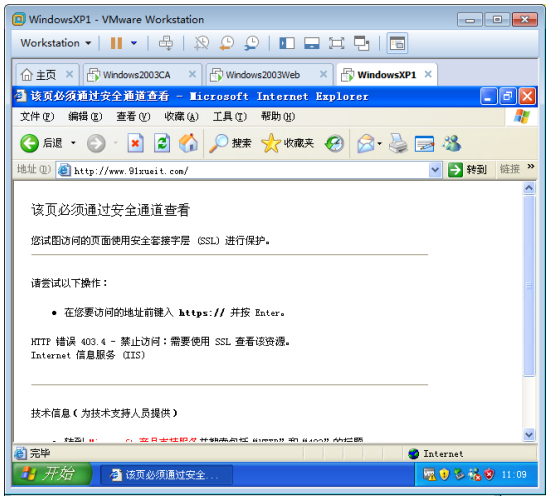

图 10-115　必须使用 https 访问

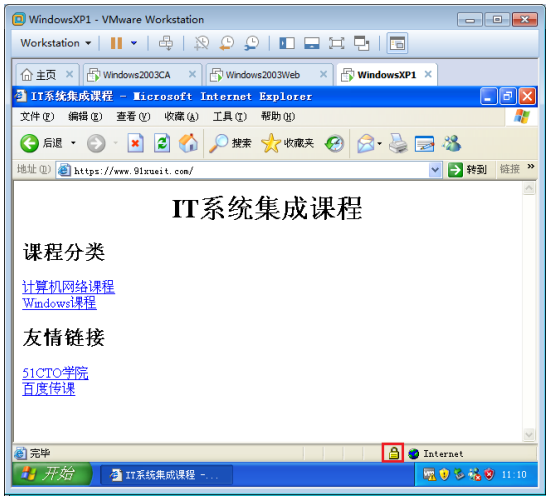

图 10-116　查看网站数字证书

如图 10-117 所示，出现 Web 站点出示的 Web 证书，在“常规”选项卡下，可以看到该证书的目的为“保证远程计算机的身份”，颁发给 www.91xueit.com 这个网站，颁发者 91xueitCA，及其有效期。

如图 10-118 所示，在“证书路径”选项卡下，可以看到是 91xueitCA 给 www.91xueit.com 颁发的证书。

如图 10-119 所示，输入 https://192.168.80.123 访问该网站，会弹出一个安全警报，提示“安全证书上的名称无效，或者与站点名称不匹配。”可以点击“查看证书”，看看网站证书中的域名是什

么。观察到证书有效期到 2017 年 9 月 13 日。

图 10-117　网站出示的数字证书

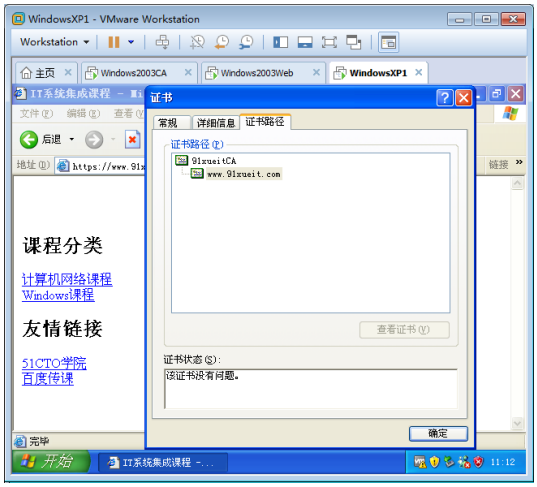

图 10-118　查看证书颁发者

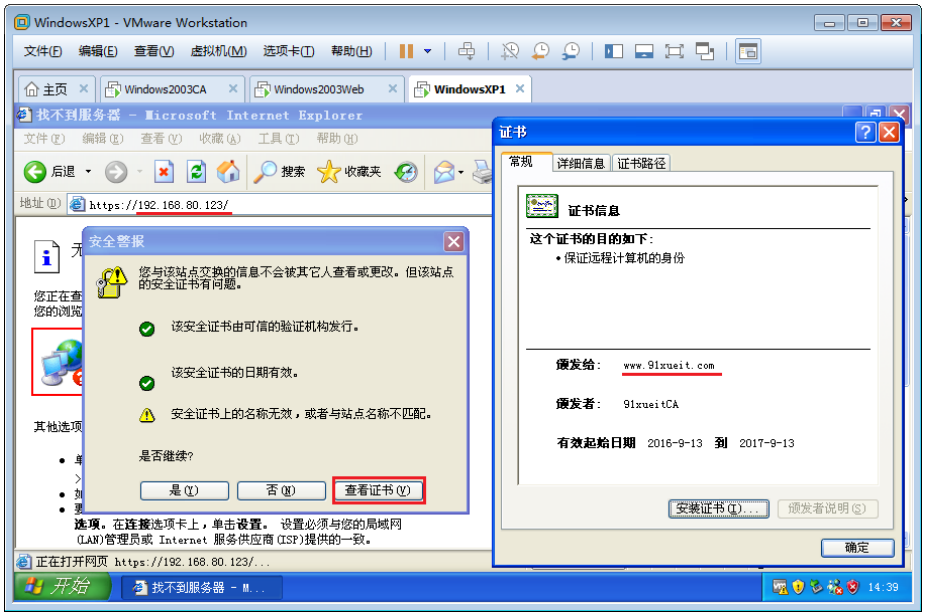

图 10-119　安全证书上的名称和访问网站的域名不一致

在“安全警报”对话框中点击“是”，照样可以通过 https 浏览网页。你和网站之间的通信依然是加密的。

如图 10-120 所示，更改 WindowsXP 的系统时间为 2018 年 9 月 13 日，再次输入 https://192.168.80.123，出现安全警报，增加了提示“该安全证书已到期或还未生效”，如图 10-121 所示。

通过上面的操作，我们学会了配置网站绑定数字证书实现和客户端的安全通信和服务器身份的确认。

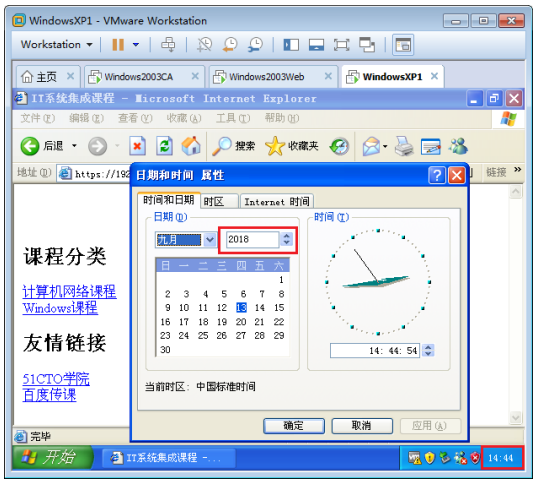

图 10-120　更改系统时间

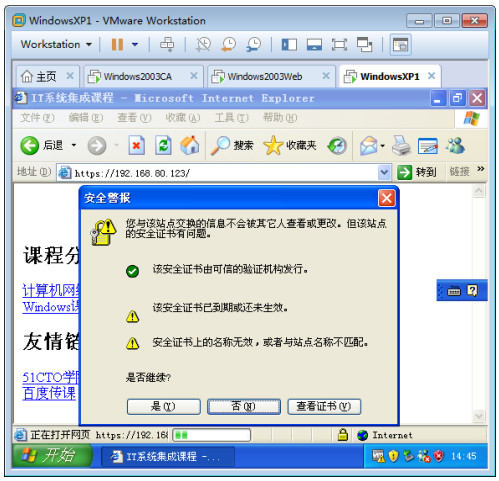

图 10-121　不在证书有效期也会出现安全警告

10.6　网络层安全 IPSec

前面讲的使用 Outlook Express 进行数字签名和数字加密，是应用层实现的安全，也就是需要应用程序来实现对电子邮件的数字签名和加密。而安全套接字实现的安全是在应用层和传输层之间插入了一层来实现数据通信的安全。

现在要讲的 IPSec 是网络层实现的安全，不需要应用程序支持，只要我们配置计算机之间通信的安全规则，传输层的数据传输单元就会被加密后封装到网络层，实现数据通信安全。IPSec 协议工作在 OSI 模型的第三层，可以实现基于 TCP 或 UDP 的协议通信安全，前面讲的安全套接字层（SSL）就不能保护 UDP 层的通信流。

10.6.1　IPSec 协议

IPSec 就是“IP 安全（Security）协议”的缩写，是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议（IP）网络上进行保密而安全的通信。IPSec 定义了在网络层使用的安全服务，其功能包括数据加密、对网络单元的访问控制、数据源地址验证、数据完整性检查和防止重放攻击。

在 IPSec 中最主要的两个协议就是：鉴别首部（Authentication Header，AH）协议和封装安全有效载荷（Encapsulation Security Payload，ESP）协议。AH 提供源点鉴别和数据完整性，但不能保密。而 ESP 比 AH 复杂得多，它提供源点鉴别、数据完整性和保密。IPSec 支持 IPv4 和 IPv6，但在 IPv6 中，AH 和 ESP 都是扩展首部的一部分。

AH 协议的功能都已包含在 ESP 协议中，因此使用 ESP 协议就可以不使用 AH 协议。但 AH 协议早已使用在一些商品中，因此 AH 协议还不能废弃。下面我们不再讨论 AH 协议，而只讨论 ESP 协议。

使用 IPSec 协议的 IP 数据报称为 IPSec 数据报，它可以在两个主机之间、两个路由器之间、或一个主机和一个路由器之间发送。在发送 IPSec 数据报之前，在源实体和目的实体之间必须创建一条网络逻辑连接，即安全关联（Security Association，SA）。

如图 10-122 所示，Client 计算机到 Web 服务器的安全关联为 SA1，Client 到 SQL 服务器的安全关联为 SA2。当然，要想实现安全通信，Web 服务器也要有到 Client 的安全关联，SQL 服务器也要有到 Client 的安全关联。

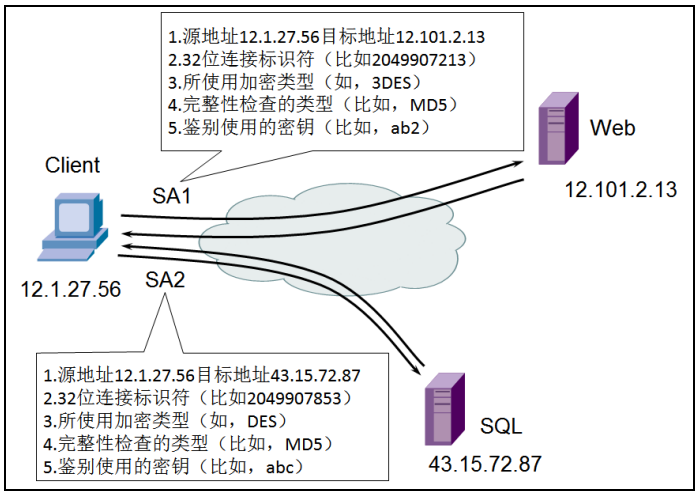

图 10-122　安全关联 SA

以 Client 计算机到 Web 服务器的安全关联 SA1 为例，来说明一条安全关联包括的状态信息。

（1）源点（Client 的 IP 地址）和终点（Web 服务器的地址）。

（2）一个 32 位的连接标识符，称为安全参数索引（Security Parameter Index，SPI）。

（3）所使用的加密类型（如 DES）。

（4）加密密钥。

（5）完整性检查类型（例如，使用报文摘要 MD5 的报文鉴别码 MAC）。

（6）鉴别使用的密钥（比如指定身份验证密钥为 abc）。

当 Client 给 SQL 服务器发送 IPSec 数据报时，就必须读取 SA1 的这些状态信息，以便知道如何对 IP 数据报进行加密和鉴别。当然 SQL 服务器也要有到 Client 的一条安全关联。

10.6.2　实战：在 Windows 系统上配置 IPSec 实现安全通信

下面在 Windows 虚拟机中配置 IPSec，实现计算机之间的安全通信。需要两个虚拟机 WindowsXP 和 Windows2003Web，WindowsXP 的 IP 地址为 192.168.80.111，Windows2003Web 的 IP 地址为 192.168.80.123。

Windows 2003 和 Windows XP 中的 IPSec（也就是 IP 安全策略）可以创建多个规则，每个规则由三部分组成：筛选器（源地址、目标地址、协议、端口号）、动作（允许、拒绝、加密通信）、和身份验证方法（Kerberos、数字证书、共享密钥）。

下面的操作就是在 Windows 2003 上创建 IP 安全策略，然后创建一个规则（源地址是 Windows 2003 的 192.168.80.123 到目标地址是 Windows XP 的 192.168.80.111），创建一个动作（加密通信，指定加密算法（3DES）和完整性算法（SHA1）），指定身份验证的共享密钥“abc123”。

在 Windows2003Web 服务器上，以管理员身份登录，点击“开始”→“程序”→“管理工具”→“本地安全策略”。如图 10-123 所示，现在我们要创建自定义的 IP 安全策略，右击“IP 安全策

略，在本地计算机”，点击“创建 IP 安全策略”。

如图 10-124 所示，在出现的“IP 安全策略名称”对话框中输入 IP 安全策略名称，点击“下一步”。

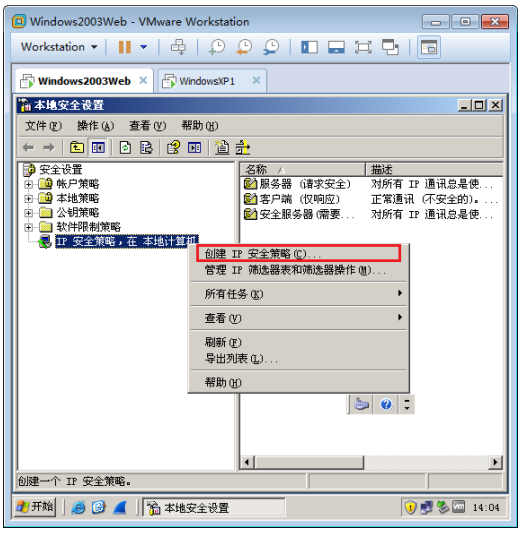

图 10-123　创建 IP 安全策略

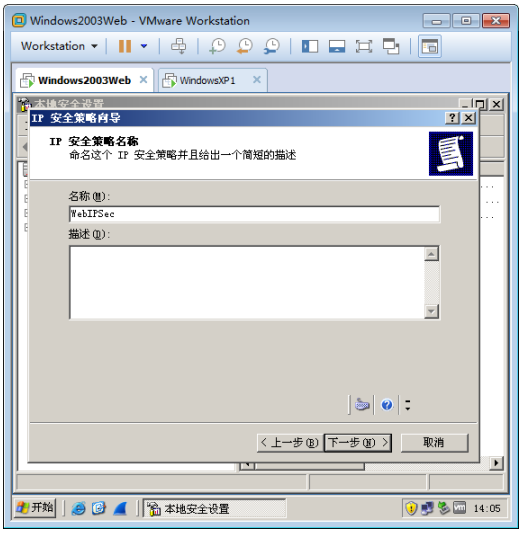

图 10-124　指定 IPSec 名称

Windows 中可以有多个 IP 安全策略，但同一时间只有一个生效，这三个默认的 IP 安全策略是对加入域的计算机预设的，在这里我们要创建自己的 IP 安全策略。

如图 10-125 所示，在出现的“安全通信请求”对话框中取消“激活默认响应规则”，点击“下一步”。

如图 10-126 所示，在出现的“正在完成 IP 安全策略向导”对话框中勾选“编辑属性”，点击“完成”。

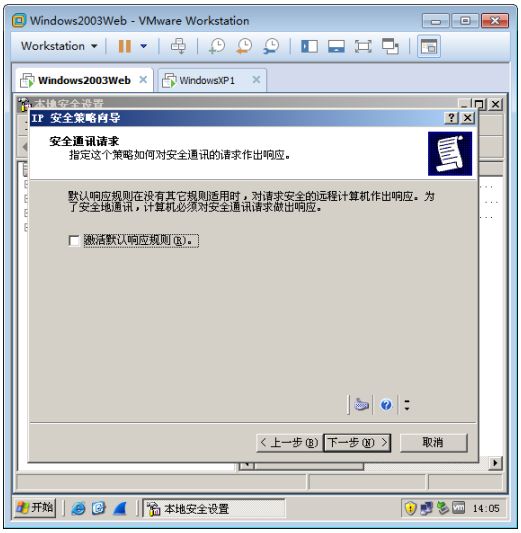

图 10-125　安全通信请求

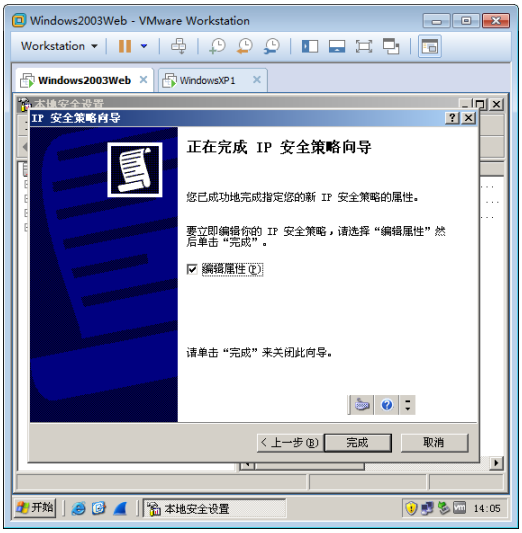

图 10-126　完成策略创建

如图 10-127 所示，在出现的“WebIPSec 属性”对话框中可以看到有一条默认规则，该规则没

被选中，不起作用。取消勾选“使用‘添加向导’”，点击“添加”。

如图 10-128 所示，在出现的“新规则属性”对话框中的“IP 筛选器列表”中，可以看到有两个预定义的筛选器。我们不使用这两个筛选器，需要创建自己的筛选器，点击“添加”。

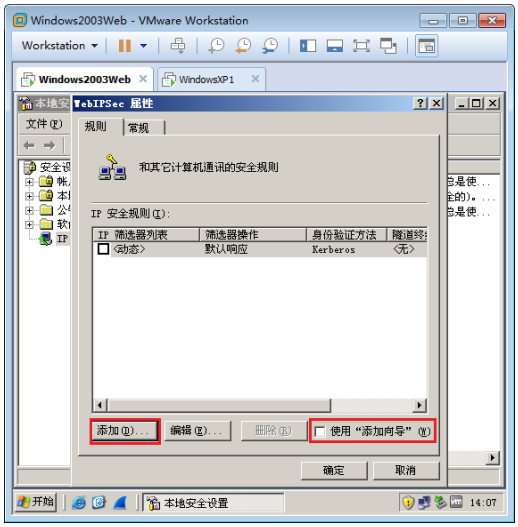

图 10-127　在策略中添加安全规则

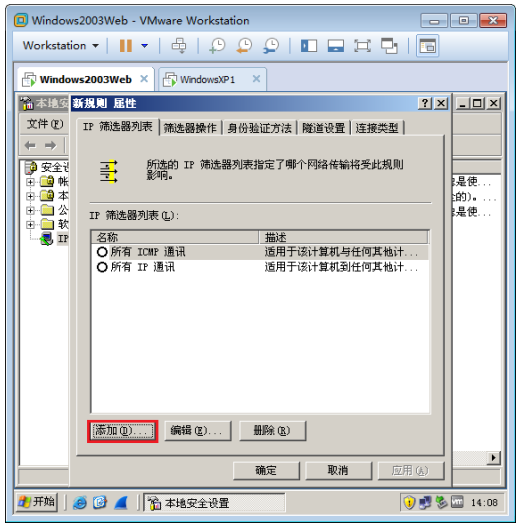

图 10-128　添加新的筛选器

筛选器，就是定义安全关联的条件，筛选器中需要指明源 IP 地址、目标 IP 地址、协议、目标端口和源端口。

如图 10-129 所示，在出现的“IP 筛选器列表”对话框中输入名称，取消勾选“使用添加向导”，点击“添加”。

如图 10-130 所示，在出现的“IP 筛选器属性”对话框中的“地址”选项卡下，源地址选择“我的 IP 地址”，目标地址选择“一个特定的 IP 地址”，输入 WindowsXP 的 IP 地址，这里一定要勾选“镜像，与源地址和目标地址正好相反的数据包相匹配”，点击“确定”。

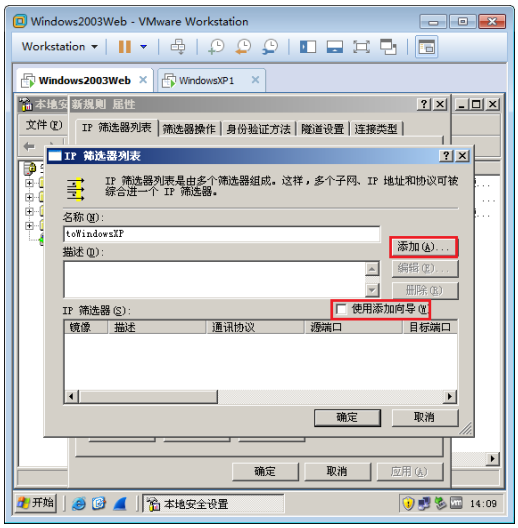

图 10-129　添加筛选器

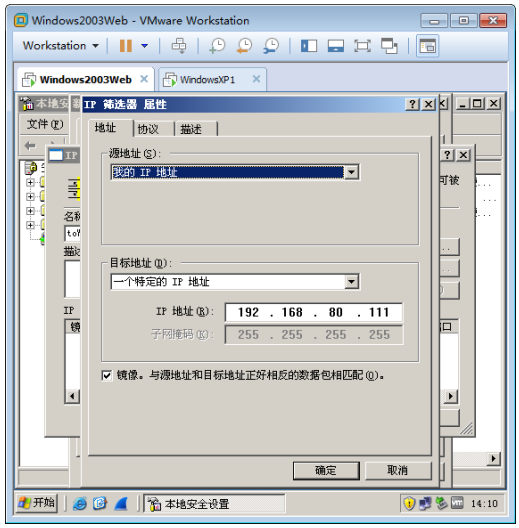

图 10-130　指定源地址和目标地址

如图 10-131 所示，在“IP 筛选器属性”对话框的“协议”选项卡下。可以选择协议、源端口和目标端口，在这里我们选择“任意”，点击“确定”。

如图 10-132 所示，在“IP 筛选器列表”对话框中还可以继续点击“添加”，添加新的 IP 筛选器，这里就添加这一条，点击“确定”。

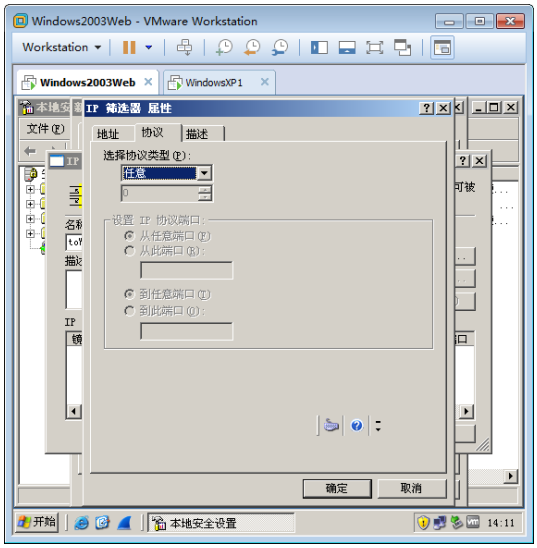

图 10-131　指定协议

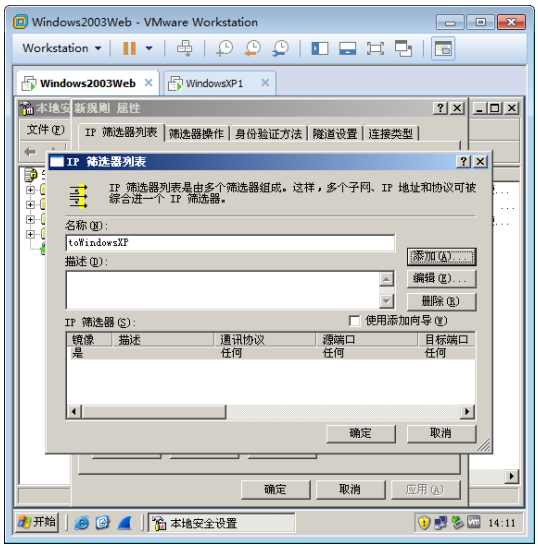

图 10-132　添加的筛选器

如图 10-133 所示，返回到“新规则属性”对话框，可以看到刚刚创建的筛选器列表，选中该筛选器。

如图 10-134 所示，在“筛选器操作”选项卡中可以看到有三个默认的筛选器操作。为了学习，我们创建自己的筛选器操作，取消勾选“使用‘添加向导’”，点击“添加”。

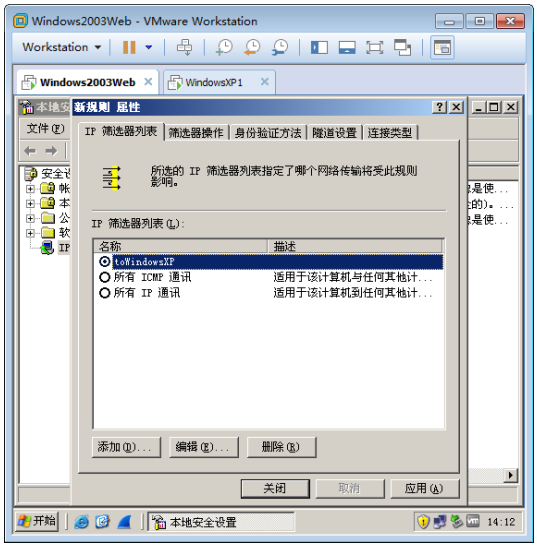

图 10-133　选定筛选器列表

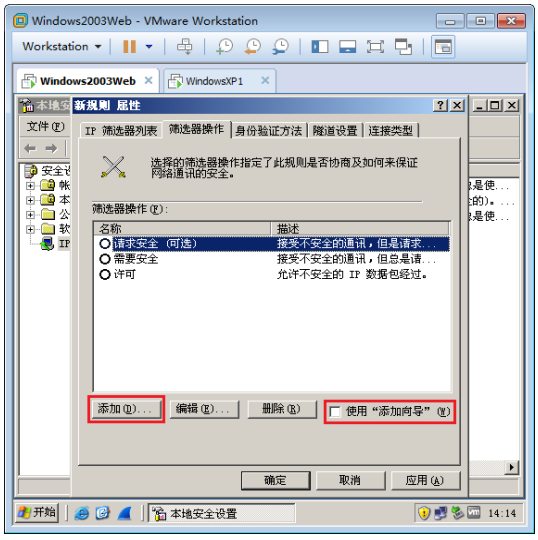

图 10-134　添加新操作

如图 10-135 所示，在出现的“新筛选器操作属性”对话框的“安全措施”选项卡下，选中“协商安全”，点击“添加”。

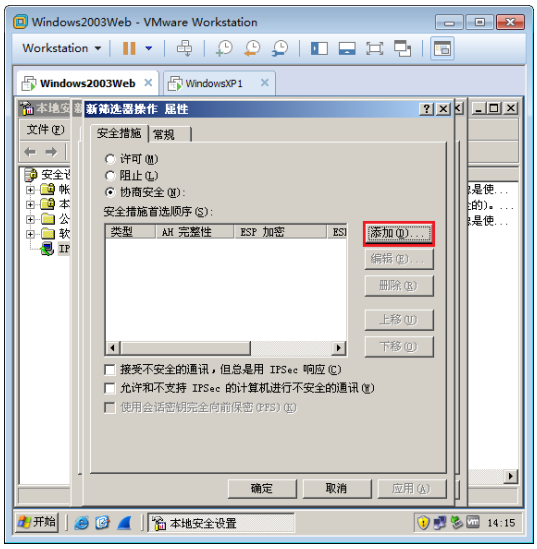

图 10-135　添加安全措施

筛选器操作有“允许”“拒绝”和“协商安全”，只有“协商安全”才需要指明加密算法和完整性算法，以及身份验证方法；如果是允许或拒绝，则不需要指定加密算法和完整性算法以及身份验证方法。

如图 10-136 所示，在出现的“新增安全措施”对话框中选中“自定义”，点击“设置”。

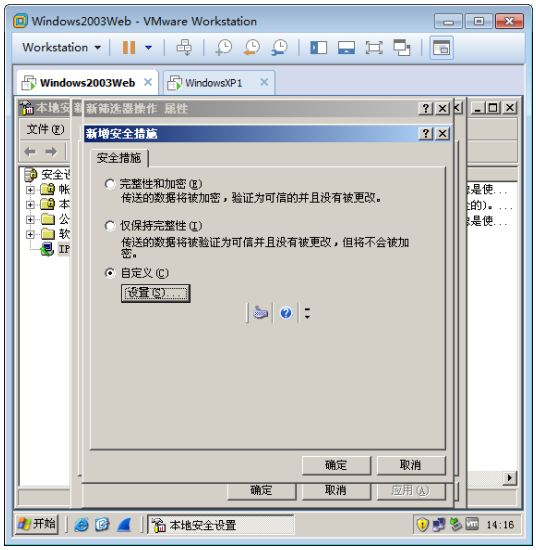

图 10-136　自定义安全措施

如图 10-137 所示，在出现的“自定义安全措施设置”对话框中勾选“数据完整性和加密”，完整性算法选中 SHA1，加密算法选中 3DES，勾选“生成新密钥间隔”和“生成新密钥间隔”。这两

个间隔，第一个指定发送了多少字节的数据，第二个指定发送了多长时间的加密数据，就会生成一个新密钥加密传输的数据。点击“确定”。

如图 10-138 所示，在“新筛选器操作属性”对话框中可以看到添加的安全措施，当然也可以添加多个安全措施，这里我们就添加这一种安全措施，勾选“接受不安全的通信，但总是用 IPSec 响应”和“使用会话密钥完全向前保密”。

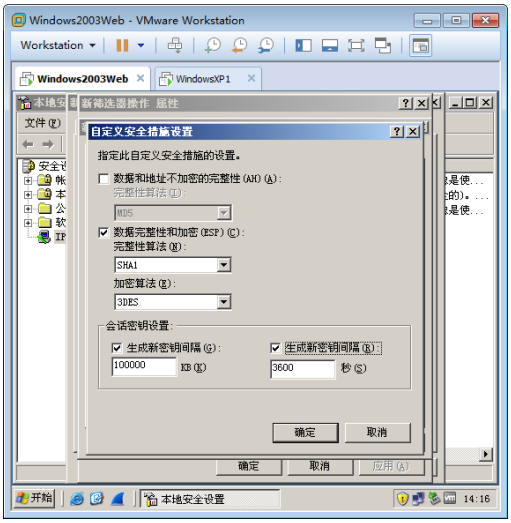

图 10-137　设置完整性和加密算法

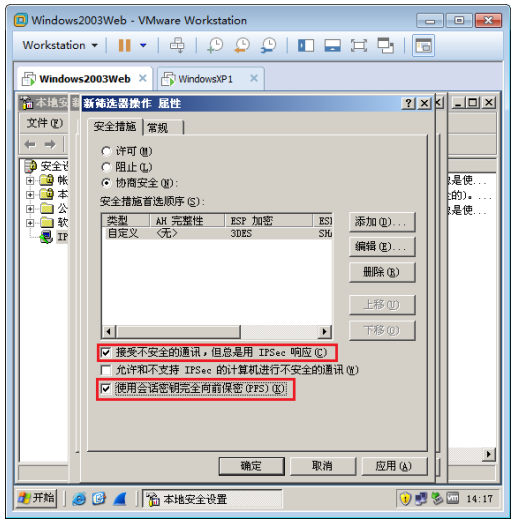

图 10-138　必须安全通信且密钥不能重复使用

勾选“接受不安全的通信，但总是用 IPSec 响应”，就意味着只允许进行安全通信；勾选“使用会话密钥完全向前保密”，通信过程生成的新的会话密钥就不会使用以前用过的会话密钥。

如图 10-139 所示，在“常规”选项卡下，输入新筛选器操作的名称，点击“确定”。

如图 10-140 所示，在“新规则属性”对话框“筛选器操作”选项卡下，可以看到刚刚创建的筛选器操作，选中创建的筛选器操作。

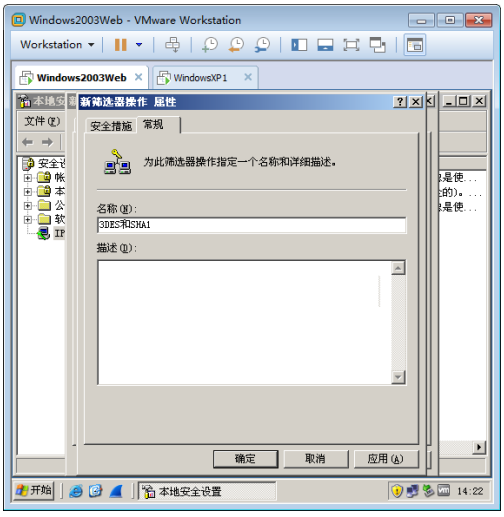

图 10-139　指定操作名称

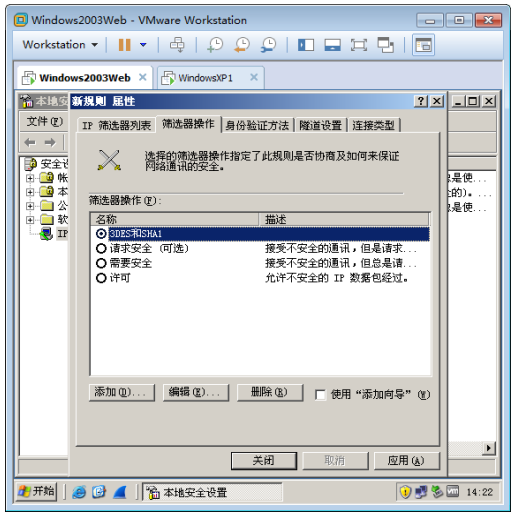

图 10-140　选择刚刚创建的操作

如图 10-141 所示，在“身份验证方法”选项卡下，可以看到有默认的方法 Kerberos，这是为域中的计算机准备的身份验证方法。现在的计算机没有加入域，我们可以编辑该身份验证方法，选中 Kerberos，点击“编辑”。

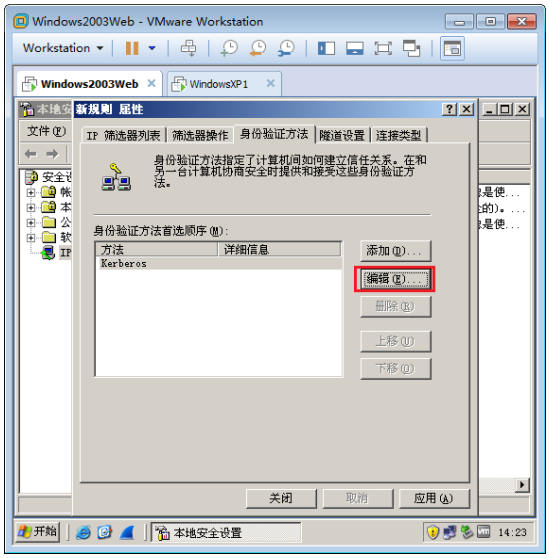

图 10-141　编辑身份验证方法

如图 10-142 所示，在出现的“身份验证方法属性”对话框中选中“使用此字符串（预共享密钥）”，输入“abc123”，点击“确定”。

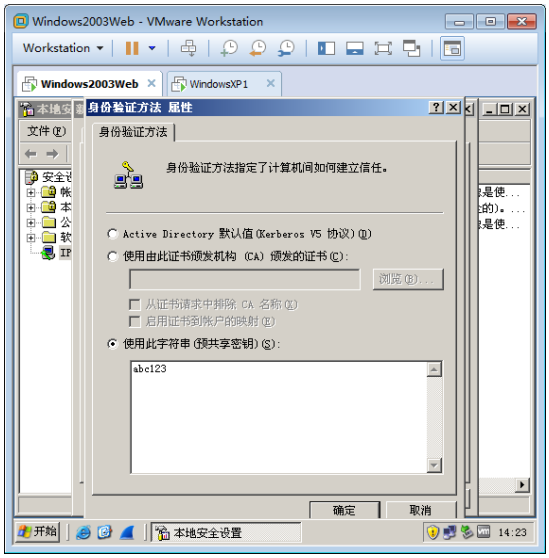

图 10-142　使用预共享的密钥

这要求在 WindowsXP 上也使用相同的密钥。

如图 10-143 所示，在“WebIPSec 属性”对话框中可以看到刚刚创建的 IP 筛选器列表、筛选

器操作和身份验证方法，点击“确定”。

> 当然，还可以继续点击“添加”，在这个 IPSec 中添加多条规则，每种规则可以指定不同的安全措施和身份验证方法。

如图 10-144 所示，右击创建好的 IPSec，点击“指派”，该策略生效。

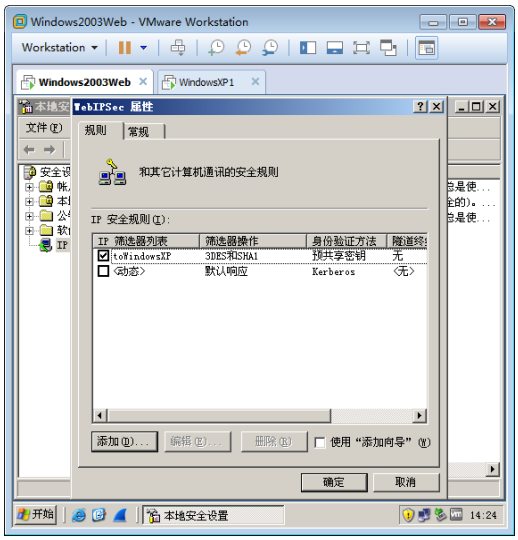

图 10-143　查看创建的安全规则

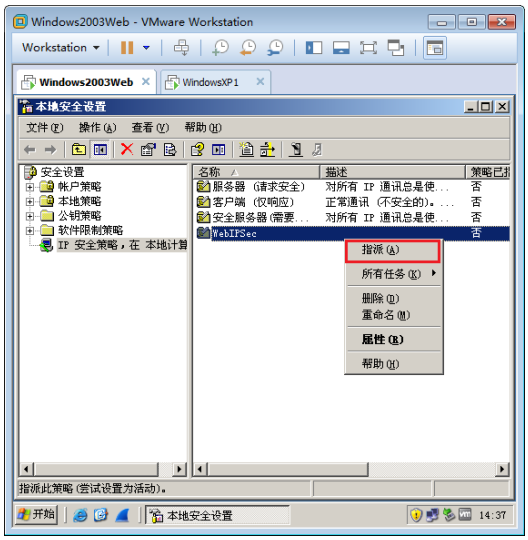

图 10-144　指派安全策略

在 WindowsXP 上点击“开始”→“运行”，输入 secpol.msc，点击“确定”，打开本地安全策略。创建新的 IPSec，如图 10-145 所示，输入 IPSec 名称，点击“下一步”。

如图 10-146 所示，参照 Windows2003Web 上的操作添加筛选器，目标地址填写 192.168.80.123，也就是 Windows2003Web 的地址。

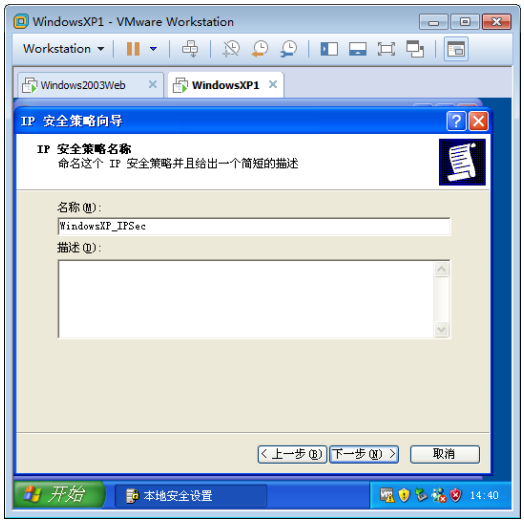

图 10-145　创建 IP 安全策略

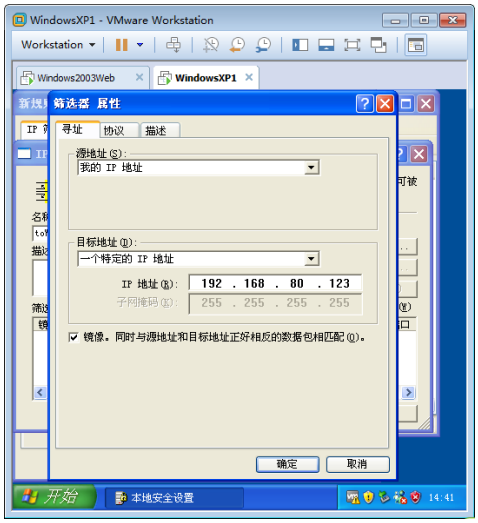

图 10-146　指定源地址和目标地址

其他的操作也参照 Windows2003Web 上的操作，创建筛选器操作和指定身份验证方法，创建完 IPSec 后，如图 10-147 所示，右击该策略，点击“指派”。

如图 10-148 所示，在 WindowsXP 上打开命令提示符，ping Windows2003Web 的 IP 地址，可以看到第一个响应是 Negotiating IP Security（协商 IP 安全），后面就从 Windows2003Web 返回了 ICMP 响应，说明 ICMP 数据包经过了 IPSec 策略，可以进行加密通信了。

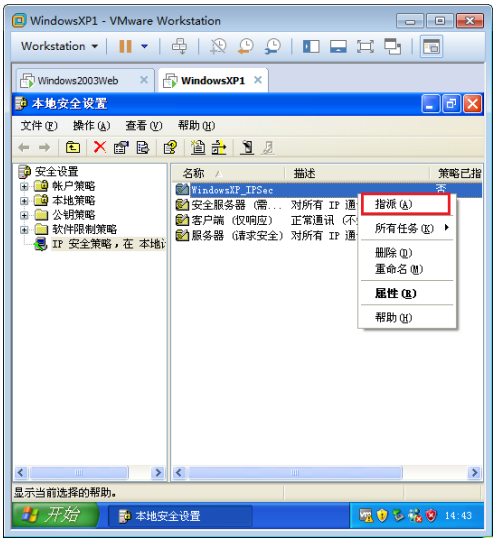

图 10-147　指派创建的 IP 安全策略

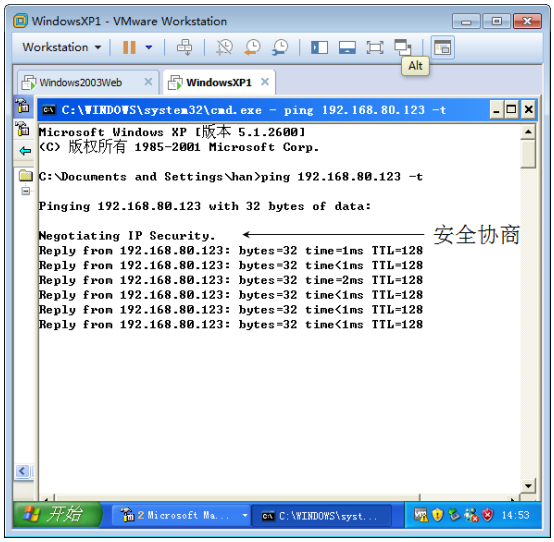

图 10-148　安全通信

10.6.3　实战：查看安全关联和加密数据包

前面讲了使用 IPSec 通信的计算机会生成安全关联 SA，记录源地址到目标地址使用的加密类型、身份验证方法等设置。下面在 WindowsXP 上查看建立的安全关联。在 Windows2003Web 上使用抓包工具，查看 IPSec 加密后的数据包，然后讲解 IPSec 数据包的格式。

如图 10-149 所示，在 WindowsXP 上点击“开始”→“运行”，输入 mmc，点击“确定”，打开微软管理控制台，点击“文件”→“添加/删除管理单元”。

> 微软管理控制台可以把多个管理工具集中到一起，也可以把没有出现在管理工具中的管理工具添加到管理控制台。

如图 10-150 所示，在出现的“添加/删除管理单元”对话框中点击“添加”，在出现的“添加独立管理单元”对话框中选中“IP 安全监视器”，点击“添加”。

如图 10-151 所示，在出现的 IP 安全监视器工具中点击“安全关联”，在右侧可以看到安全关联。

在 Windows2003Web 上安装抓包工具，捕获加密的数据包，如图 10-152 所示，可以看到加密后的数据包网络层协议号变为 50，网络层封装的内容已经被加密，称为“封装安全有效载荷（ESP）”，只能看到 SPI（安全索引参数）和 ESP Sequence（序号）。

可以看到使用 IPSec 加密后的数据包，但不能看到传输首部和应用层封装的内容，因此没办法判断该数据包使用的是什么协议和什么端口。

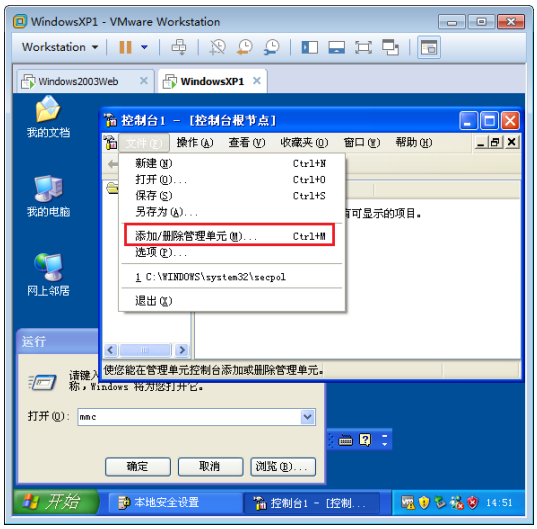

图 10-149　添加管理单元

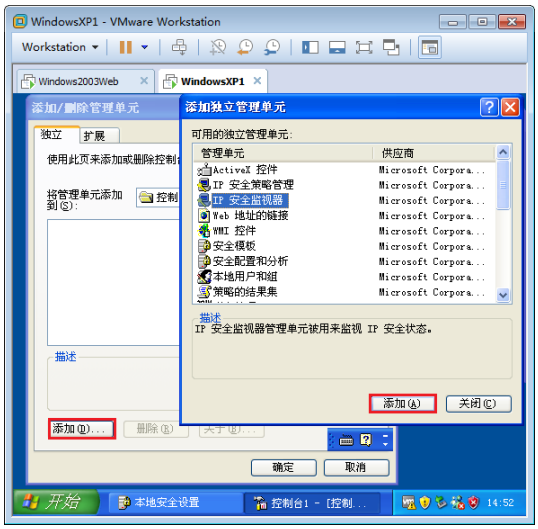

图 10-150　添加 IP 安全监控器

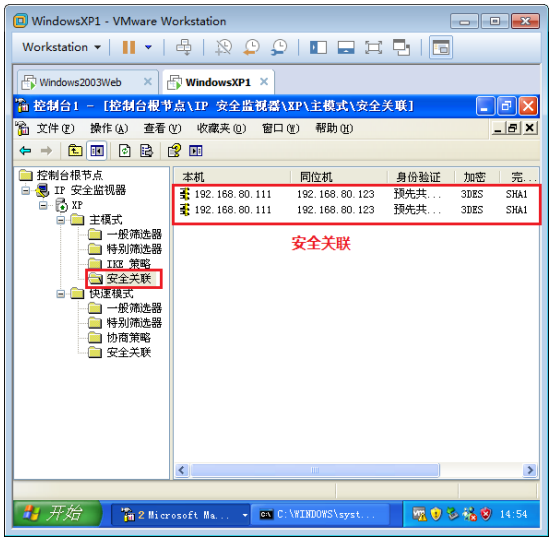

图 10-151　查看安全关联 SA

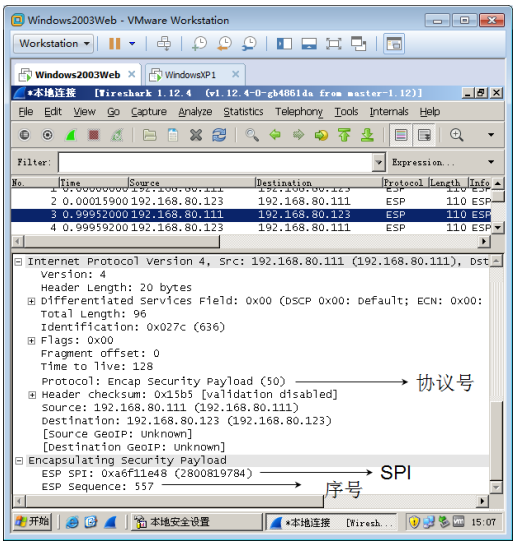

图 10-152　查看 IPSec 加密的数据包

IPSec 数据包的格式如图 10-153 所示。

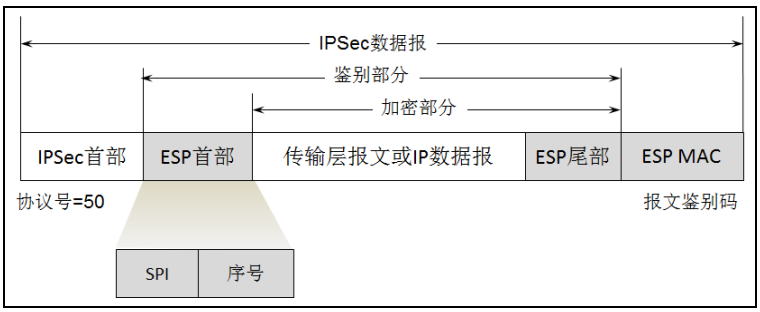

图 10-153　IPSec 数据包格式

使用 ESP 时，IP 数据报首部的协议字段置为 50。当目的主机检查到协议字段是 50 时，就知道在 IP 首部后面紧接着的是 ESP 首部。

同时在原 IP 数据报后面增加了两个字段，即 ESP 尾部和 ESP 数据。在 ESP 首部中，有标志一个安全关联的安全参数索引 SPI（32 位）和序号（32 位）。

ESP 尾部和传输层报文（或 IP 数据报）一起进行加密，因此攻击者无法得知所使用的传输层协议（它在 IP 数据报的数据部分中）。

按照 SA 指明的算法和密钥，对“ESP 首部+传输层报文段（或 IP 数据报）+ESP 尾部”生成报文鉴别码 MAC。

因此，用 ESP 封装的数据报既有鉴别源点和检查数据报完整性的功能，又能提供保密。

习题

1．计算机网络都面临哪几种威胁？主动攻击和被动攻击的区别是什么？对于计算机网络的安全措施都有哪些？

2．试解释以下名词：（1）截获；（2）拒绝服务：（3）篡改：（4）流量分析；（5）恶意程序。

3．对称密钥体制与公钥密码体制的特点各如何？各有何优缺点？

4．公钥密码体制下的加密和解密过程是怎样的？为什么公钥可以公开？如果不公开是否可以提高安全性？

5．试述数字签名的过程。

6．因特网的网络层安全协议族 IPSec 都包含哪些主要协议？

7．试简述 SSL 和 SET 的工作过程。

8．实战：配置两个虚拟机之间使用 IPSec 加密通信，身份验证方法使用预共享密钥。

9．实战：在一个虚拟机安装证书颁发机构，另一个虚拟机搭建 Web 服务器，为 Web 站点申请数字证书，配置强制使用 https 通信。

10．实战：申请两个 sohu.com 电子邮箱，安装证书颁发机构，为电子邮箱用户申请证书，发送签名和加密的电子邮件，并导出数字证书（包含私钥）。