教学课题：数据安全

教学目的要求：1、明确两种数据加密技术的异同点。

2、明确数字签名技术的使用方法及作用

3、掌握数据加密与数字签名的区别与联系。

教学重点：1、对称加密技术和非对称加密技术

2、数字签名技术

3、数据加密和数字签名的区别与联系

课时：2 课时

教学过程：

数据安全

一、数据的加密技术

（一）数据加密技术概述

1、数据加密技术的概念：

所谓数据加密技术是指将一个信息（或称明文）经过加密钥匙及加密函数转换，变成无意义的密文，而接收方则将此密文经过解密函数、解密钥匙还原成明文。

通过对信息进行加密，实现信息隐蔽，从而起到保护信息的安全的作用。加密技术是网络安全技术的基石。

2、与加密技术相关的几个术语

1）明文：是指没有加密的信息，可以直接理解其含义。明文可以是文本、语音、图像、视频等。

2）密文：通过加密手段，将明文变换成晦涩难懂的信息，称为密文。

3）加密过程：将明文转换成密文的过程。

4）解密过程：加密的逆过程，即将密文转换成明文的过程。

5）密码体制：加密和解密过程都是通过特定的算法来实现的，这一算法称为密码体制。

6）密钥：把明文和密文相互转换使用的钥匙，将明文转换密文使用的钥匙称为加密密钥，反之称为解密密钥。

（二）两种数码加密技术

加密技术分对称性加密技术（密钥加密）和非对称性加密技术（公钥加密）

对称数据加密技术，加密和解密采用同一把密钥，所以对称。因这种加密技术采用同一把钥匙，所以称这把钥匙为密钥，故又称为密钥加密技术。（注意只有一把钥匙，叫密钥），这种加密技术以 DES 为典型。

非对称数据加密技术，加密和解密采用不同密钥，所以才非对称。在这种加密技术中，有两把钥匙，一把叫公钥（这把钥匙是公开的），一把叫私钥（这把钥匙是不公开的），使用公钥加密，私钥解密，所以又称为公钥加密技术。这种加密技术以 RSA 为典型。

对称加密技术，加密和解密的算法公开，但密钥不公开（都公开就没意义了）。

非对称加密技术，加密和解密的算法公开，公钥公开，只有私钥不公开（也不能公开）。

对称数据加密技术的实现过程：甲给乙发送信息，发送前，甲用自己的密钥将明文通过加密算法转换成密文，然后发送出去，乙收到密文后需要用密钥进行解密，而密钥是不公开的，只有甲知道，乙不知道，所以甲还需要将密钥发送给乙，如果密钥在发送过程中被截获，则信息就会被破解，所以这种加密技术可靠性不是很高。

非对称数据加密技术的实现过程：甲给乙发送信息，发送前，甲用乙的公钥将明文通过加密算法转换成密文（公钥是公开的），然后发送出去，乙收到密文后用自己的私密钥进行解密，而乙的私钥就在自己手里，所以不用传送，所以这种加密技术可靠性很高。但这种加密技术算法复杂，加密后得到的密文变长，速度慢（比对称加密慢 10~100 倍），所以用的不是很多。

（三）两种加密技术的联系：

数字加密常采用对称加密和非对称加密相结合的方法，这是因为：

对称加密速度快，适于加密大量数据；非对称加密速度慢（比对称加密慢 10~100 倍），且加密后得到的密文变长，只适于加密小数据。如果 A 向 B 传输大量的数据，一般传输数据时采用对称加密技术，因对称加密技术中加密密钥和解密密钥是一样的，A 还要向 B 传送密钥，为了保证密钥传送的安全性，这个密钥的传送需要采用非对称加密技术，这样更可靠。

二、数字签名技术

（一）数字签名：

发送报文时，发送方（甲）用一个 hash 算法从报文中产生固定长度的报文摘要，然后利用自己的私钥对这个摘要进行加密，这个过程就叫签名。这个加密后的摘要作为报文的数字签名和报文一起发送给接收方。接收方用发送方（甲）的公钥解密被加密的摘要（报文附加的数字签名）得到结果 A，然后用和发送方一样的 hash 算法从接收到的原始报文中算出报文摘要 B。最后,把 A 和 B 作比较。如果相同，那么接收方就能确认该信息的确是甲发过来的。（因为加密和解密必须是一对密钥，接收方用甲的公钥解密，如果解出的 A 和接收方自己产生的 B 相同，就说明当初一定是甲的私钥的加密，即发送方一定是甲，也就确定了发送者的身份，可以防抵赖，当然如果 A 和 B 不一样，就可以断定要么不是甲发送的，要么就是数据被篡改了，故数字签名还能确认数据是否被修改，即数据的完整性。）

所以数字签名的功能是：对发送者（签名者）进行身份认证；保证信息的完整性；防止交易中的抵赖发生。

（二）数字签名与加密的区别与联系

1、区别：

数字签名的功能:

a) 对签名者进行身份认证;

b) 保证信息的完整性（在交易过程中，没有被篡改）

c) 防止交易中的抵赖发生（签名者无法否认信息是由自己发出的）

加密的功能：

a)重点在于“数据的安全性”，即保密性，可以防止数据被监听攻击。

2、联系：数字签名技术中也使用加密技术。数字签名只采用了非对称密钥加密算法，数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密。而数据加密采用了对称密钥加密算法和非对称密钥加密算法相结合的方法，它能保证发送信息保密性。且非对称加密技术用的是接收方的密钥对，即加密时用接收方的公钥加密，解密时用接收方的私钥解密，过程正好相反。

三、数据压缩技术：

个人认为，数据压缩技术与数据安全关系不是很大，但数据压缩后能防病毒，防病毒也是数据安全的一部分。随着计算机通信网络的剧增，使得网络上传输的数据量非常大，显然数据压缩技术能够大大减少存储和通信费用，这才是数据压缩最重的意义。我们常用的压缩工具很多，如 WinRAR、WinZip 、 Gzip 等。

四、数据备份：数据备份和数据安全密切相关，如果我们养成备份数据的习惯，数据被破坏后，可以随机恢复数据。

数据备份，按照备份时所备份数据的特点，可以分为完全备份、增量备份和系统备份 3 种。

完全备份，把指定目录下的所有数据都进行备份，且用存储空间很大，一般只是系统第一次运行时备份一次。

增量备份，是数据有变动或数据变动达到指定的数据值才对数据进行的备份，只备份增量部分，占用存储空间小，要经常进行。

系统备份，是对整个系统进行备份，占用空间也很大，一般是每隔几个月或一年左右进行一次。

大型的服务器这些备份通过设置，可自动进行。

五、习题分析

1. 为使发送方不能否认自己发出的签名消息，应该使用（ ）技术

A). 数据加密　　B). 防火墙

C). 链路加密　　D). 数字签名

标准答案:d

解析：

保证信息传输的完整性、发送者的身份确认、防止交易中的抵赖发生。

数字签名技术中也使用加密技术。数字签名只采用了非对称密钥加密算法，数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密。而数据加密即可采用对称密钥加密算法，也能采用非对称密钥加密算法。其非对称加密技术用的是接收方的密钥对，即加密时用接收方的公钥加密，解密时用接收方

的私钥解密，过程正好与数字签名相反。

2、对称数据加密技术中，加密和解密过程采用不同的两把密钥，通信双方都必须各自具备这两把钥匙，并且保证不被泄漏。

正确

错误

标准答案:b

解析：

对称数据加密技术，加密和解密采用同一把密钥，所以才对称，又称为密钥加密技术。

非对称数据加密技术，加密和解密采用不同密钥，所以才非对称，在这种加密技术中，使用公钥加密，私钥解密，所以又称为公钥加密技术。

对称加密技术，加密的算法公开，但密钥不公开（都公开就没意义了）。

非对称加密技术，加密的算法公开，公钥公开，只有私钥不公开（也不能公开）。

非对称加密技术，加解密用的是接收方的密钥对，接收方收到数据后使用自己的私钥解密，别人无法解密，所以能保证数据的安全性。

数字签名技术，数字签名部分使用发送方的私钥加密，接收方收到数据后使用发送方的公钥（公开的，都能知道）解密验证。因为私钥只有你自己有，所以它可以保证数据只能是你发出的，不可能有别人发出，从而实现发送者身份认证、防止交易中抵赖的发生。当然数字签名还能保证信息传输的完整性。

3. 数字签名可以保证消息内容的机密性。

A). 正确　　B). 错误　　（正确率 16%）

标准答案:b

解析：

数字签名保证信息传输的完整性、发送者的身份确认、防止交易中的抵赖发生。不保证消息内容的机密性，要想保证其机密性可以在发送时进行加密。

4. 加密和解密过程均采用同一把密钥，通信时双方都必须具备这把钥匙的技术是（　　）

A). 对称数据解密技术　　B). 非对称数据解密技术

C). 对称数据加密技术　　D). 非对称数据加密技术

标准答案:c

解析：

加密技术有在对称数据加密技术和非对称加密技术。

前者又称为密钥加密技术（只有一把钥匙，叫密钥，千万别说成私钥加密，回为根本就没有私钥），后者又称为公钥加密技术（有两把钥匙，公钥和私钥，公钥加密，私钥解密）这两种技术中，加密和解密算法都是公开的。

对于密钥加密技术（前者），只有一个密钥（即加密和解密采用同一把钥匙），且密钥不公开，这种技术加密和解密是对称的，以 DES 为典型。

而对于非对称密码技术（后者），使用不同的加密密钥与解密密钥，加密密钥（即公钥）是向大众公开的，而解密密钥（即私钥）是需要保密的，这种技术加密和解密是不对

称的，以 RSA 为典型。

5. 以下关于 VPN 说法正确的是（）

A). VPN 只能提供身份认证，不能提供加密数据的功能。

B). VPN 指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路。

C). VPN 不能做到信息认证和身份认证

D). VPN 指的是用户通过公用网络建立的临时的、安全的连接

标准答案:d

6. 数字签名是数据的接收者用来证实数据的发送者身份确认无误的一种方法，目前常采用的数字签字标准是（ ）

A). CRC 标准　　B). DSS 标准

C). SNMP 标准　　D). DSA 标准

标准答案:b

解析：

DSS：数字签名标准（DigitalSignatureStandard）美国政府用来指定数字签名算法的一种标准。DSA 是数字签字算法

7. 以下哪一项不是预防计算机病毒的措施？　（　　）

A). 专机专用　B). 不上网　C). 建立备份　D). 定期检查

标准答案:b

解析：

建立备份，一旦发中毒，可以恢复备份，减少损失。

专机专用，没有交叉感染，可以减少中毒机会

定期检查，及早发现清除减少损失。

不上网那叫因噎废食，怕中毒，就不上网了，干脆别用电脑了。

8. 下列文件中属于压缩文件的是()。

A). trans.doc　　B). test.zip

C). map.htm　　D). fit.ext

标准答案:b

解析:压缩文件的扩展名一般是 rar 或 zip。