数据加密技术

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。

数据加密意义

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。

数据加密技术

- 1、对称性加密技术（密钥加密）
- 2、非对称性加密技术（公钥加密）

两种加密技术的特点

- 1、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）
- 2、 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）
- 3、两种加密技术的算法都是公开的。

两种加密技术的实现过程

- 对称加密技术：
- 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

两种加密技术的实现过程

- 非对称加密技术：
- 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。

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。

数字签名技术

- 何为数字签名：
  - 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

- 1、对发送者（签名者）进行身份认证
- 2、保证信息的完整性
- 3、防止交易中的抵赖发生

数字签名与加密的区别

一、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）

数字签名与加密的区别

二、加密的功能：

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。

数字签名与加密的联系

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。

习题分析

1. 数字签名中也要用到加密技术，且用的是非对称加密技术，但数字签名是用（C）的（B）加密，用（C）的（A）解密；而一般的非对称加密技术，是用（D）的（A）加密，用（D）的（B）解密。

A). 公钥　B). 私钥　C). 发送方　D). 接收方

习题分析

2. 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

答案:d

3、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

答案:b

习题分析

4. 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%）

答案:B

5. 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

答案:C

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). DES标准　D). RSA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。

结束语

本课到此结束

感谢同学们的配合