电子商务技术基础

第五章 电子商务安全

第五章 电子商务安全

- 第一节 电子商务的安全需求
- 第二节 信息的保密性技术
- 第三节 数据完整性技术
- 第四节 不可否认技术
- 第五节 身份认证技术

第一节 电子商务的安全需求

- 由于病毒、黑客攻击、用户帐号被盗和网页内容被恶意篡改等情况，产生了电子商务的四大安全需求：
  - 信息安全需求
  - 信用安全需求
  - 管理安全需求
  - 法律保证安全需求
- 电子商务安全应具备的几个基本安全特征：
  - 信息的保密性；
  - 信息的完整性；
  - 信息的不可否认性；
  - 交易者身份的真实性；
  - 系统的可靠性、可用性、可控性。

第一节 电子商务的安全需求

1、电子商务安全的基本要求

- 保密性—保障个人的、专用的和高度敏感数据的机密。电子商务系统应该对主要信息进行保护，阻止非法用户获取和理解原始数据。
- 认证性—电子商务系统应提供通讯双方进行身份鉴别的机制，确认通信双方的合法身份。可以通过数字签名和数字证书相结合的方式实现用户身份的验证，证实他就是他所声称的那个人。数字证书应由可靠的证书认证机构签发，用户申请数字证书时应提供足够的身份信息，证书认证机构在签发证书时应对用户提供的身份信息进行真实性认证。
- 完整性—电子商务系统应该提供对数据进行完整性认证的手段，保证所有存储和管理的信息不被篡改。

第一节 电子商务的安全需求

1、电子商务安全的基本要求

- **授权**—电子商务系统需要控制不同的用户谁能够访问网络上的信息并且能够进行何种操作。
- **数据原发者鉴别**—电子商务系统应能提供对数据原发者的鉴别，确保所收到的数据确实来自原发者。这个要求可以通过数据完整性及数字签名相结合的方法来实现。
- **可访问性**—保证系统、数据和服务能被合法地访问。
- **防御性**—能够阻挡不希望的信息或黑客。

第一节 电子商务的安全需求

1、电子商务安全的基本要求

- 数据原发者的不可抵赖和不可否认性—电子商务系统应能提供数据原发者不能抵赖自己曾做出的行为，也不能否认曾经接到对方的信息，这在交易系统中十分重要。
- 合法用户的安全性—合法用户的安全性是指合法用户的安全性不受到危害和侵犯，电子商务系统和电子商务的安全管理体系应该实现系统对用户身份的有效确认、对私有密匙和口令的有效保护、对非法攻击的有效防范等。
- 网络和数据的安全性—电子商务系统应能提供网络和数据的安全，保护硬件资源不被非法占有，软件资源免受病毒的侵害。

第一节 电子商务的安全需求

2、电子商务安全内容

- 电子商务安全从整体上可分为两大部分：计算机网络安全和商务交易安全,两者相辅相成，缺一不可。
- 计算机网络安全包括：计算机网络设备安全、计算机网络系统安全、数据库安全等。其特征是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，以保证计算机网络自身的安全性为目标。
- 商务交易安全紧紧围绕传统商务在互联网络上应用时产生的各种安全问题，在计算机网络安全的基础上，如何保障电子商务过程的顺利进行。即实现电子商务的保密性、完整性、可鉴别性、不可伪造性和不可抵赖性。

第五章 电子商务安全

- 第一节 电子商务的安全需求
- **第二节 信息的保密性技术**
- 第三节 数据完整性技术
- 第四节 不可否认技术
- 第五节 身份认证技术

第二节 信息的保密性技术

- 两大信息保密技术
  - 加密/解密技术（针对信息本身）
  - 防火墙技术（针对信息的传递途径）

第二节 信息的保密性技术

1、密码学(Cryptology)

- crypto- 表示“隐秘”之义
- 密码编码学 Cryptography

  编制密码以保护秘密信息，是密码体制的设计学。
- 密码分析学 Cryptoanalysis

  研究加密信息的破译以获取消息, 即在未知密钥的情况下，密文推出明文或密钥的技术。
- 密码编码学和密码分析学合起来称为密码学。

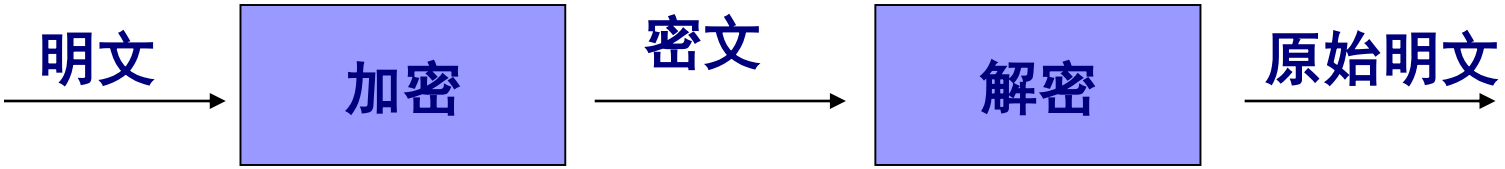
第二节 信息的保密性技术

2、加密/解密技术

- 是一种用来防止信息泄露的技术，主要概念包括：
  - 加密(Encryption)：为了防止信息的内容被他人有意或无意的知晓，需要将它的内容通过一定的方法转变成别人看不懂的信息，这个过程就是加密。
  - 解密(Decryption)：将看不懂的信息再转变还原成原始信息的过程称为解密。
  - 明文(Plain text)：加密之前的信息被称为明文。
  - 密文(Encryption text)：加密之后的内容称为密文。
  - 密钥：加密通常要采用一些算法（对应着加密/解密的程序），而这些算法需要用到不同的参数，这些不同的参数称作密钥。
  - 密钥空间：所有密钥的集合。

第二节 信息的保密性技术

2、加密/解密技术



明文P：消息的初始形式

密文C：加密后的形式

加密： $C=E_k(P)$，E为加密算法

解密： $P=D_k(C)$，D为解密算法

满足： $P=D(E(P))$

K 密钥

第二节 信息的保密性技术

3、加密/解密的类型

- 按保密程度
  - 理论上保密的加密
  - 实际上保密的加密
  - 不保密的加密
- 按照密钥使用方式
  - 对称加密：加密密钥、解密密钥可以相互推算得出，或者干脆是相同的，$P=D_k(E_k(P))$，如DES算法。
  - 非对称加密：加密、解密密钥不相同，不能推算，$P=D_{kd}(KD,E_{ke}(P))$，如RSA算法。

第二节 信息的保密性技术

3、加密/解密的类型

- 按照密钥使用方式分类

对称加密方法

方法	描述
DES()	是美国国家标准局1970s开发的一种对称加密算法，采用分组乘积密码体制。数据块64位，密码64或56位。
IDEA()	由瑞士苏黎士联邦工业大学的赖学嘉和James L.Massey于1990年共同提出。数据块64位，密码长128位。
FEAL()	日本NTT公司的清水和宫口设计
Rijndael(荣代尔)	一种高级的加密标准(AES)，由比利时Joan Daemen和Vincent Rijmen提出，用于代替DES,其数据块长度和密钥长度可分别为128、192、256。
RC	

非对称加密方法

RSA	由MIT的Ron rivest、Adi Shamir、Leonard Adleman于1978年提出。安全性基础是数论和计算复杂性理论中的下述论断：“求两个大素数(>10^100)的乘积在计算上是容易的，但若要分解两个大素数的积而求出它的因子则在计算上是困难的”
EL Gamal	1985年由EL Gamal提出，安全性基于“在有限域上计算离散对数比计算指数更高的困难”(DLP)。
背包系统	第一种出现的公开钥加密算法，由Ralph Merkle和Martin Hellman于1978年基于求解背包问题的难解性而提出的。
McEliece	1978年由McEliece提出。基于“将一个译码容易的线性码经过变换而伪装成一个译码困难的线性码”原理。
Diffe-Hellman	1976年出现，安全性基于“在有限域上计算离散对数比计算指数更高的困难”
椭圆曲线密码(FEE、ECC)	1985年由N.Koblitz和V.Miller提出，利用有限域上的椭圆曲线上点集所构成的群，在其上定义离散对数系统。安全性基于“在有限域上计算离散对数比计算指数更高的困难”。

第二节 信息的保密性技术

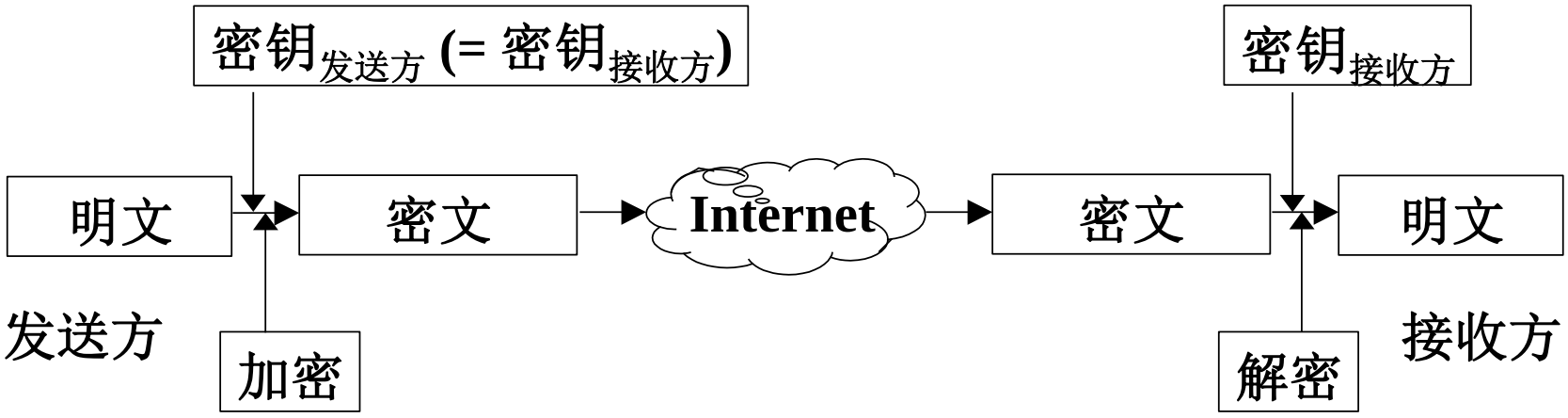
4、对称加密

- 也称为单钥加密、共享密钥加密或机密密钥加密，收发双方拥有相同的单个密钥，这把密钥既可用于加密，也可用于解密，即加密和解密使用的是相同的一把密钥，此密钥又称为对称密钥或会话密钥。
- 常见的对称加密方法有DES、3DES、AES等。
- 对称加密算法将明文按一定的位长分组，输出也是固定长度的密文。

第二节 信息的保密性技术

4、对称加密

- 发送方用自己的私有密钥对要发送的信息进行加密。
- 发送方将加密后的信息通过网络传送给接收方。
- 接收方用发送方进行加密的那把私有密钥对接收到的加密信息进行解密，得到信息明文。

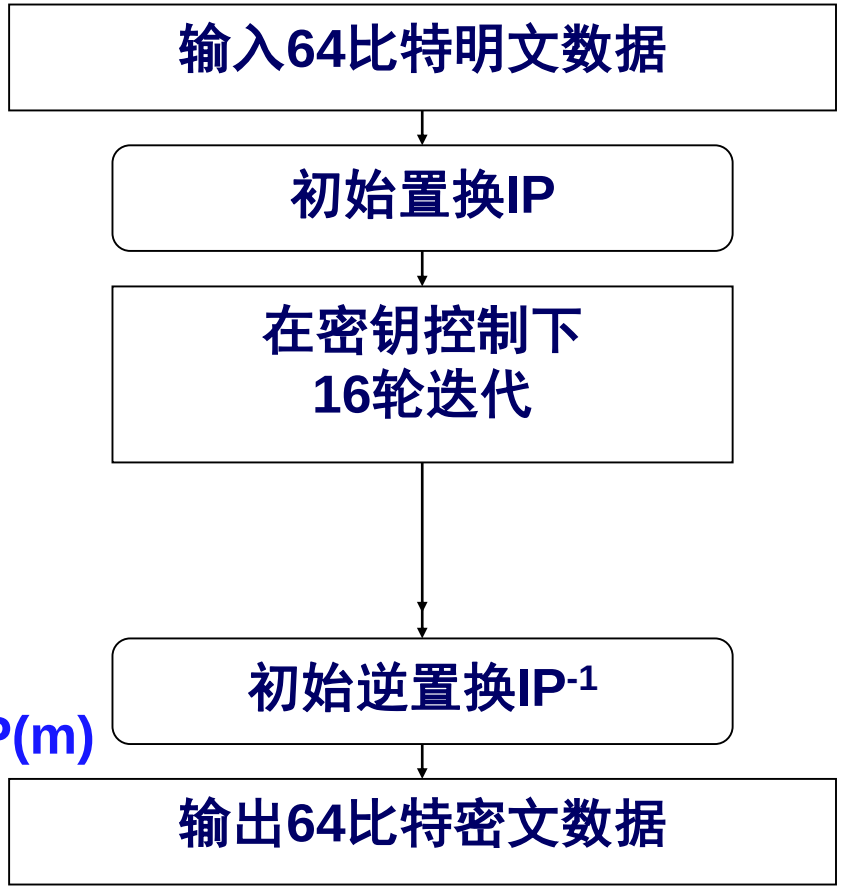


第二节 信息的保密性技术

4、对称加密

DES算法基本原理

- DES采用64位长度的数据块和56位长度的密钥。在56位密钥控制下，将64位明文块变换为64位密文块。
- 64比特的密钥中含有8个比特的奇偶校验位，所以实际有效密钥长度为56比特 。



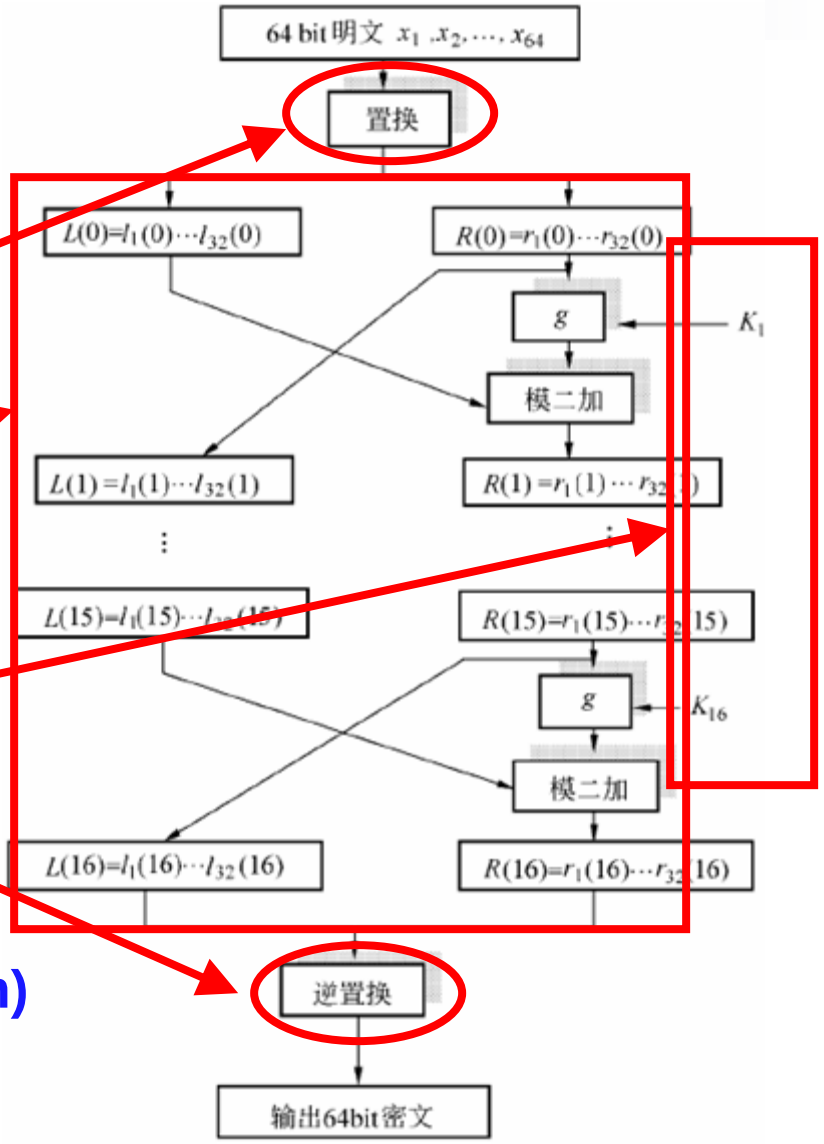
$E_K(m)=IP^{-1}\times T_{16} \times T_{15} \times \ldots \times T_1 \times IP(m)$

第二节 信息的保密性技术

4、对称加密

DES算法基本原理

- 算法大致分成四个部分：
  - 初始置换
  - 迭代过程
  - 逆置换
  - 子密钥生成



$E_K(m)=IP^{-1}\times T_{16} \times T_{15} \times \ldots \times T_1 \times IP(m)$

第二节 信息的保密性技术

4、对称加密

DES加密体制特点

- 主要优点是加密和解密速度快，加密强度高，且算法公开。
- 其最大的缺点是实现密钥的秘密分发困难，对于具有n个用户的网络，需要n(n－1)/2个密钥。在大量用户的情况下密钥管理复杂，而且无法完成身份认证等功能，不便于应用在网络开放的环境中。

第二节 信息的保密性技术

5、非对称加密

- 又称为公开密钥加密（简称公钥加密），需要采用两个在数学上相关的密钥对——公钥(public key)和私钥(private key)，对信息进行加解密。
- 在操作过程中，公钥可向外界发布，让其他人知道，私钥则自己保存，只有自己知道。
- 用公钥加密的密文只能用私钥解密，反之，用私钥加密的密文只能用公钥解密。
- 常见的非对称加密：RSA算法。
- 能够有效解决对称密钥存在的问题，即密匙分发的风险和保密的问题。

第二节 信息的保密性技术

5、非对称加密

RSA加密体制

- 基于大整数因子分解这一著名的数学难题。
- 明文分组M<N，密文C，密钥对e, d。
- 加密 $C=M^e \bmod N$
- 解密 $M=C^d \bmod N$

第二节 信息的保密性技术

5、非对称加密

模运算

- 若a=b+k×n对某些整数k成立，则a=b mod n。
- a mod n=b ←→ a≡b mod n
- 若a和b是正的，a<n，则可将a看作b被n整除后的余数。
  - 例如：2=9 mod 7
- 通常，0<=b<n，k>0。

第二节 信息的保密性技术

5、非对称加密

模运算

- 模递归运算是“模除求余”，计算 $a=k\times n+b$
- 例：
  - 33 mod 7

    33 mod 7 = (4×7 + 5) mod 7

    因此 33 = 5 mod 7
  - -18 mod 7

    -18 mod 7 = (-3×7 + 3) mod 7

    因此 -18 = 3 mod 7

第二节 信息的保密性技术

5、非对称加密

RSA加密体制

- 加密 $C=M^e \bmod N$
- 解密 $M=C^d \bmod N$
- 例1：已知明文M=85，利用(N,e)=(143,7)计算密文。

$$C=M^e \bmod N = 85^7 \bmod 143=123$$

- 例2：收到密文y=123，私钥d=103， N=143，求明文。

$$M=C^d \bmod N =123^{103} \bmod 143=85$$

第二节 信息的保密性技术

5、非对称加密

RSA算法优缺点

- 优点：能适应网络的开放性要求，密钥管理简单，并且可方便地实现数字签名和身份认证等功能，是目前电子商务等技术的核心基础。
- 缺点：算法复杂，加密数据的速度和效率较低，只能对小批量的数据进行加密。

第二节 信息的保密性技术

5、非对称加密

两种加密方法的联合使用

- 在实际应用中，通常将对称加密算法和非对称加密算法结合使用：
  - 利用对称加密算法来进行大容量数据的加密；
  - 采用RSA等非对称加密算法来传递对称加密算法所使用的密钥。
- 通过这种方法可以有效地提高加密的效率并能简化对密钥的管理。

第二节 信息的保密性技术

5、非对称加密

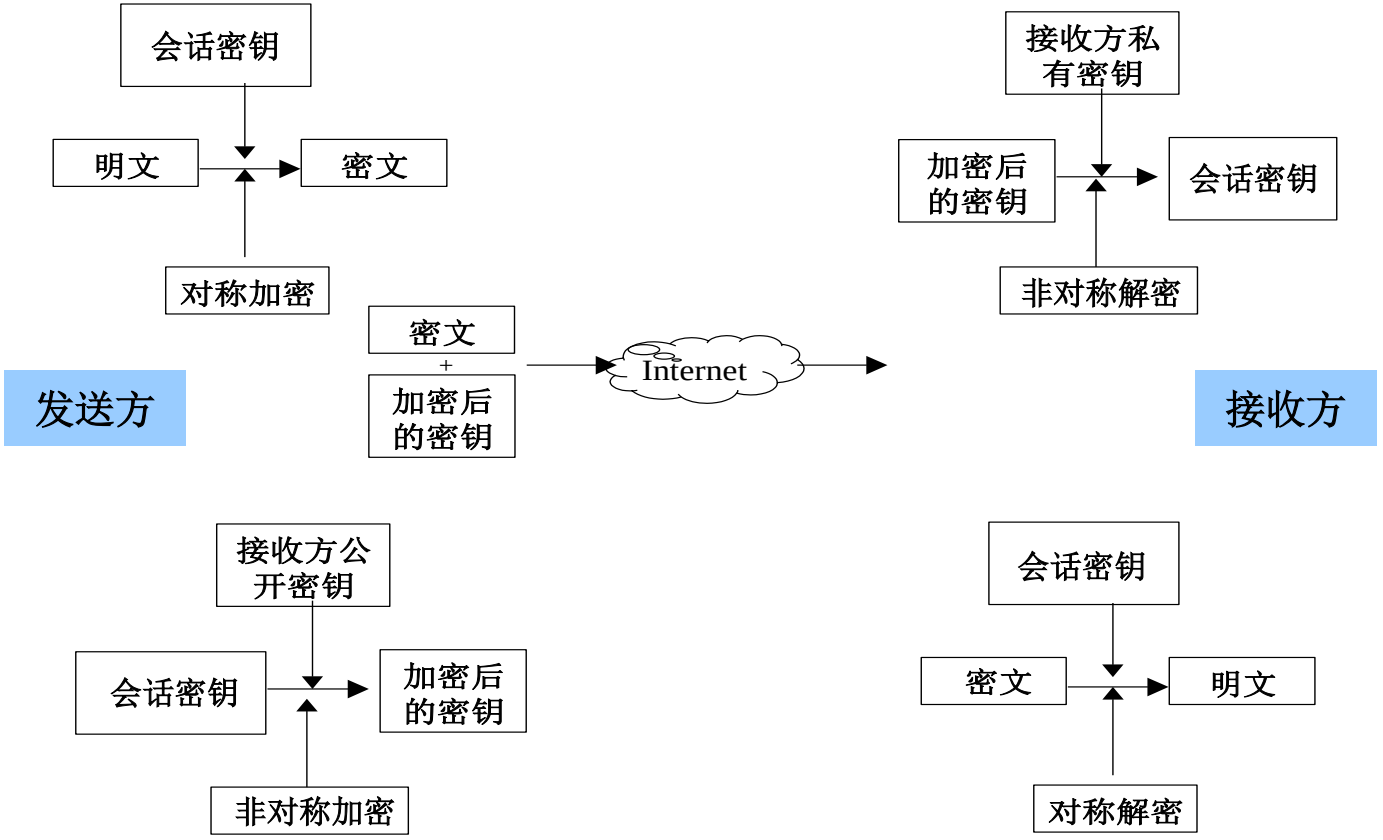
两种加密方法的联合使用

- 两个加密过程：
  - 消息流加密——发送方生成一个会话密钥，并用它对消息进行加密。(对称加密)
  - 秘密密钥加密——发送方利用接收方的公开密钥对会话密钥加密。(非对称加密)
- 两个解密过程：
  - 接收方用自己的私有密钥进行解密后得到会话密钥。
  - 用会话密钥对消息密文进行解密，得到明文。

第二节 信息的保密性技术

5、非对称加密

两种加密方法的联合使用



第二节 信息的保密性技术

6、防火墙技术

- 实现保密的另外一种方法是进行存取访问控制，对敏感数据的访问实行身份验证，具备合法身份的允许其访问，不合法身份的禁止其访问，防火墙技术正是为实现这一目的而产生的。
- “防火墙”是一种形象的说法, 其实它是一种由计算机硬件和软件的组合, 使互联网与内部网之间建立起一个安全网关，从而保护内部网免受非法用户的侵入。
- 防火墙是一个把互联网与内部网（通常这局域网或城域网）隔开的屏障。

第二节 信息的保密性技术

6、防火墙技术

防火墙的安全策略有两种：

- 没有被列为允许访问的服务都是被禁止的：需要确定所有可以被提供的服务以及它们的安全特性，开放这些服务；将所有其它未列入的服务排斥在外，禁止访问。
- 没有被列入禁止访问的服务都是被允许的：首先确定那些被禁止的、不安全的服务，以禁止它们被访问；而其它服务则被认为是安全的，允许访问。

第二节 信息的保密性技术

6、防火墙技术

防火墙分类

- 按工作原理分为两大类型：
  - 包过滤型
  - 代理服务器型（应用网关型）
- 按实现方式分为两大类型：
  - 硬件防火墙
  - 软件防火墙

第二节 信息的保密性技术

6、防火墙技术

包过滤防火墙

- 包过滤技术根据站点的安全规则，通过对数据包的检测决定是否将数据包发往目的地址，从而达到对进入和流出网络的数据进行监测和限制的目的。
- 包过滤技术工作在网络层和传输层，它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则从数据流中丢弃。

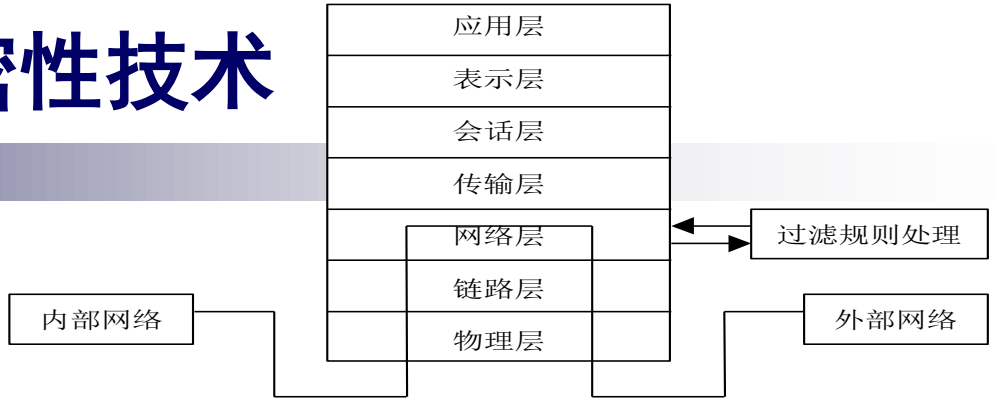
第二节 信息的保密性技术

6、防火墙技术

包过滤防火墙

- 很多路由器都支持这种功能，普通路由器与包过滤路由器间的区别表现为：
  - 普通路由器只工作在网络层，检查每个数据包的目标地址，为数据包选择最佳路由。
  - 包过滤路由器对数据包的检查更仔细，除了决定该数据包能否被它路由到目标地址之外，过滤路由器还要决定是否应该对这个包进行路由。
- 是否对这个包进行路由是依据站点的安全规则而定的，站点可依据自己的安全规则来配置路由器。

第二节 信息的保密性技术



6、防火墙技术

包过滤防火墙

- 对包依次使用规则检查，规则定义在访问控制表ACL里，操作方式有转发、丢弃、报错、备忘等。
- 通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，或通过检查它们的组合来决定是否允许该数据包通过。

Direction	Type	Src	Port	Dest	Port	Action
传输方向	协议类型	报文源地址	源主机端口	报文宿地址	宿主机端口	控制操作

第二节 信息的保密性技术

6、防火墙技术

包过滤防火墙

- 优点：成本低廉、操作简单、方便、处理速度快、透明性好，对网络性能影响不大。
- 缺点：
  - 人工决定规则配置策略，容易造成安全漏洞，且过滤规则的完备性难以得到检验，复杂过滤规则的管理也比较困难
  - 缺乏用户日志和审计信息，不保证内容的安全
  - 缺乏用户认证机制，不提供认证服务
  - 不能动态打开和关闭FPT等服务端口
  - 不能防止IP欺骗和拒绝服务攻击。
- 包过滤型防火墙的安全性较差。

第二节 信息的保密性技术

6、防火墙技术

代理服务器型防火墙

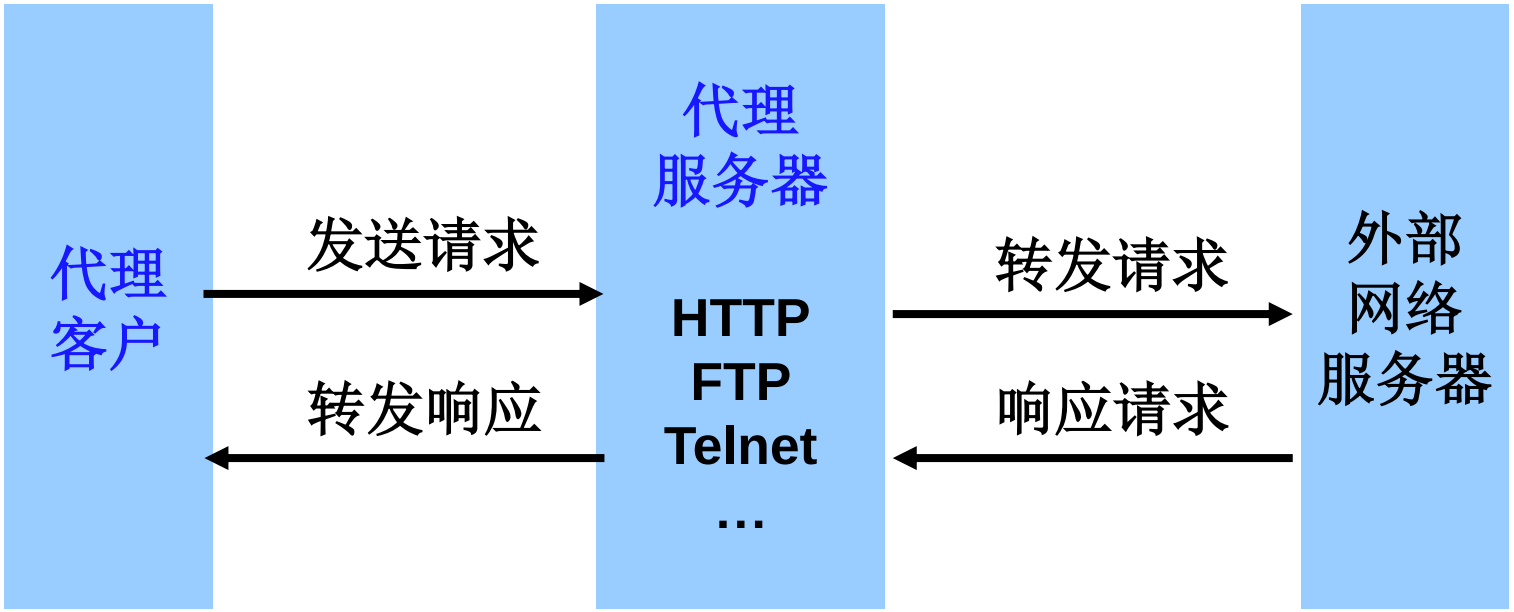
- 运行于防火墙主机上的一些特定的应用程序或者服务器程序，代替了用户与互联网的连接，被称为应用层网关。
- 包括代理服务器和代理客户两个部件。在防火墙主机上运行代理服务进程，通过该进程代理用户完成TCP/IP功能。外网和内网连接必须通过代理服务器中转。
- 代理服务能够在应用层进行用户级认证、详细日志等功能和对具体协议及应用的过滤，并能抵御拒绝服务攻击。

第二节 信息的保密性技术

6、防火墙技术

代理服务器型防火墙

- 包括代理服务器和代理客户两个部件。



第二节 信息的保密性技术

6、防火墙技术

代理服务器型防火墙

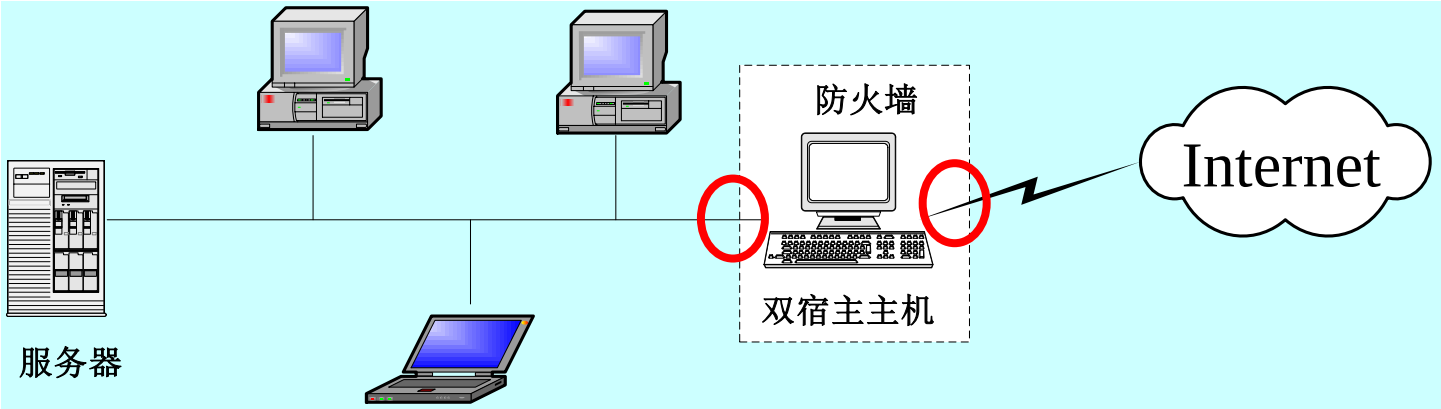
- 优点：可以将被保护的网络内部结构屏蔽起来，增强网络的安全性；能实施较强的数据流监控、过滤、记录和报告，完全控制网络信息的交换，控制会话过程，具有灵活性和安全性。
- 缺点：可能影响网络的性能，对用户不透明，且对每一种服务器都要设计一个代理模块，建立对应的网关层，实现起来比较复杂。

第二节 信息的保密性技术

7、防火墙体系结构

双宿主主机结构

- 双宿主主机的防火墙系统由一台装有两张网卡的堡垒主机构成。两张网卡分别与外部网以及内部受保护网相连。
- 双宿主主机只有用代理服务的方式或者用让用户每次都直接注册到双宿主主机上的方式，才能提供安全控制服务。



双宿主主机防火墙结构示意图

第二节 信息的保密性技术

7、防火墙体系结构

双宿主主机结构

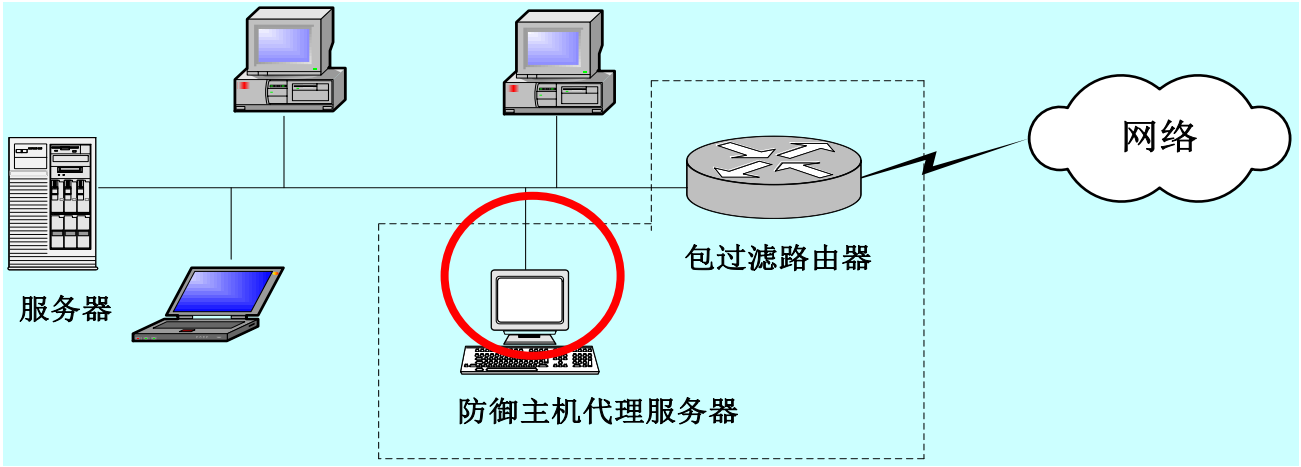
- 特点：IP通信被完全阻止。
  - 防火墙内部的系统能与双宿主主机通信，同时防火墙外部的系统（在因特网上）能与双宿主主机通信。
  - 但是内外网络之间不可直接通信，内外部网络之间的IP数据流被双宿主机完全切断。
- 双宿主主机可以提供很高程度的网络控制。

第二节 信息的保密性技术

7、防火墙体系结构

主机过滤结构

- 组成结构：由过滤路由器和运行网关软件的堡垒主机构成。提供安全保护的堡垒主机仅与内部网络相连，而过滤路由器位于内部网络和外部网络之间。



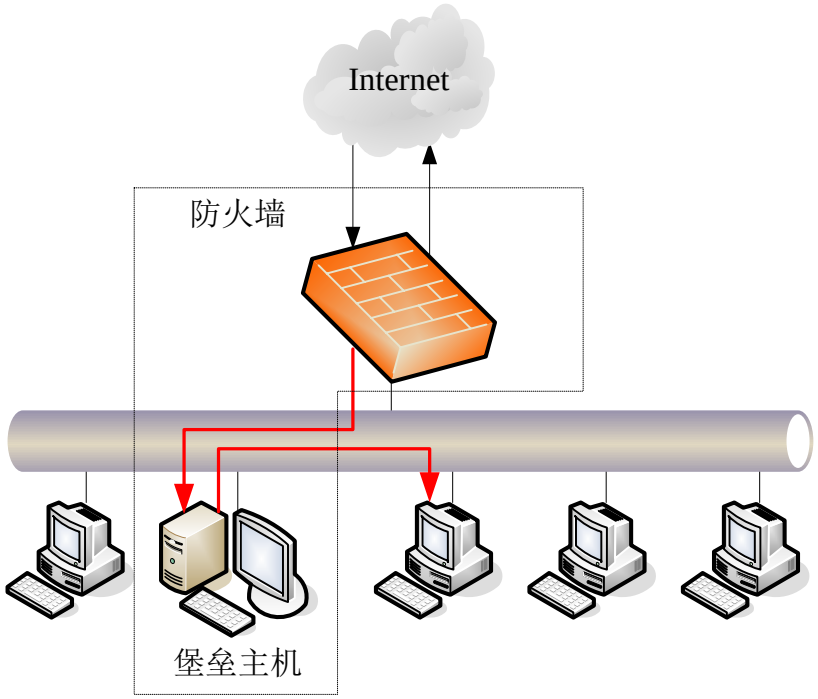
主机过滤防火墙结构示意图

第二节 信息的保密性技术

7、防火墙体系结构

主机过滤结构

- 专门设置一个过滤路由器，把所有外部到内部的连接都路由到堡垒主机上，强迫所有的外部主机与一个堡垒主机相连，而不让它们直接与内部主机相连。



第二节 信息的保密性技术

7、防火墙体系结构

主机过滤结构

- 与包过滤结构的比较：
  - 其提供的安全等级比包过滤防火墙系统要高，实现了网络层安全(包过滤)和应用层安全(代理服务)。
  - 入侵者在破坏内部网络的安全性之前，必须首先渗透两种不同的安全系统。
  - 即使入侵者进入了内部网络，也必须和堡垒主机竞争。

第二节 信息的保密性技术

7、防火墙体系结构

主机过滤结构

- 优点：可完成多种代理，还可以完成认证和交互作用，能提供完善的Internet访问控制。比双宿主机结构能提供更好的安全保护区，同时也更具有可操作性。
- 缺点：堡垒主机是网络的“单失效点”，也是网络黑客集中攻击的目标，安全保障仍不理想。只要入侵者设法通过了堡垒主机，对入侵者来讲，整个内部网与堡垒主机之间就再也没有任何阻碍。

第五章 电子商务安全

- 第一节 电子商务的安全需求
- 第二节 信息的保密性技术
- **第三节 数据完整性技术**
- 第四节 不可否认技术
- 第五节 身份认证技术

第三节 数据完整性技术

1、数据完整性方法

- 数字摘要技术
- 数字签名技术
  - 除了能保证完整性，还能有效防止交易者的交易抵赖，保证交易的不可否认。

第三节 数据完整性技术

2、数字摘要技术

- 在信息安全技术中经常需要验证消息的完整性，消息摘要函数就提供了这一服务。它是一种散列(Hash)变换，能对不同长度的输入信息产生固定长度的输出即一个单独的128、256位的大数。这个大数称为原消息的“消息摘要”或“散列”。

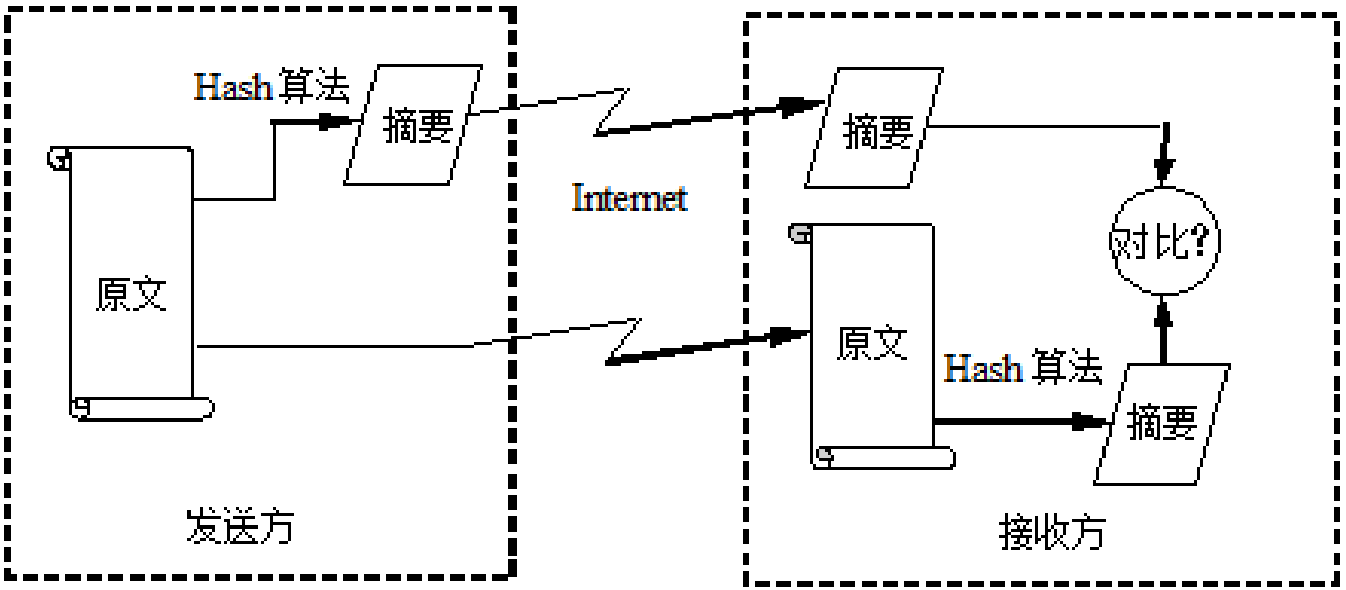
$$h=H(m)$$

- 由于消息摘要函数比对称加密算法的速度还快，因此有着广泛的应用。消息摘要函数是数字签名和消息识别码(MAC)的基础。
- 目前使用的消息摘要函数有MD5、HMAC、SHA等。

第三节 数据完整性技术

3、消息摘要应用模式

- 采用单向Hash函数（如SHA，MD5等）对要传送的信息内容进行某种变换运算，得到固定长度的摘要信息。



第五章 电子商务安全

- 第一节 电子商务的安全需求
- 第二节 信息的保密性技术
- 第三节 数据完整性技术
- **第四节 不可否认技术**
- 第五节 身份认证技术

第四节 不可否认技术

1、数字签名基本概念

- 假定A发送一个认证的信息给B，双方之间的争议可能有多种形式：
  - B伪造一个不同的消息，但声称是从A收到的；
  - A可以否认发过该消息，B无法证明A确实发了该消息。
- 数字签名就是主要用于对数字信息进行的签名，以防止信息被伪造或篡改等。与加密不同，数字签名的目的是为了保证信息的完整性和真实性，其必须保证以下三点：
  - 接受者能够核实发送者对消息的签名。
  - 发送者事后不能抵赖对消息的签名。
  - 接受者不能伪造对消息的签名。

第四节 不可否认技术

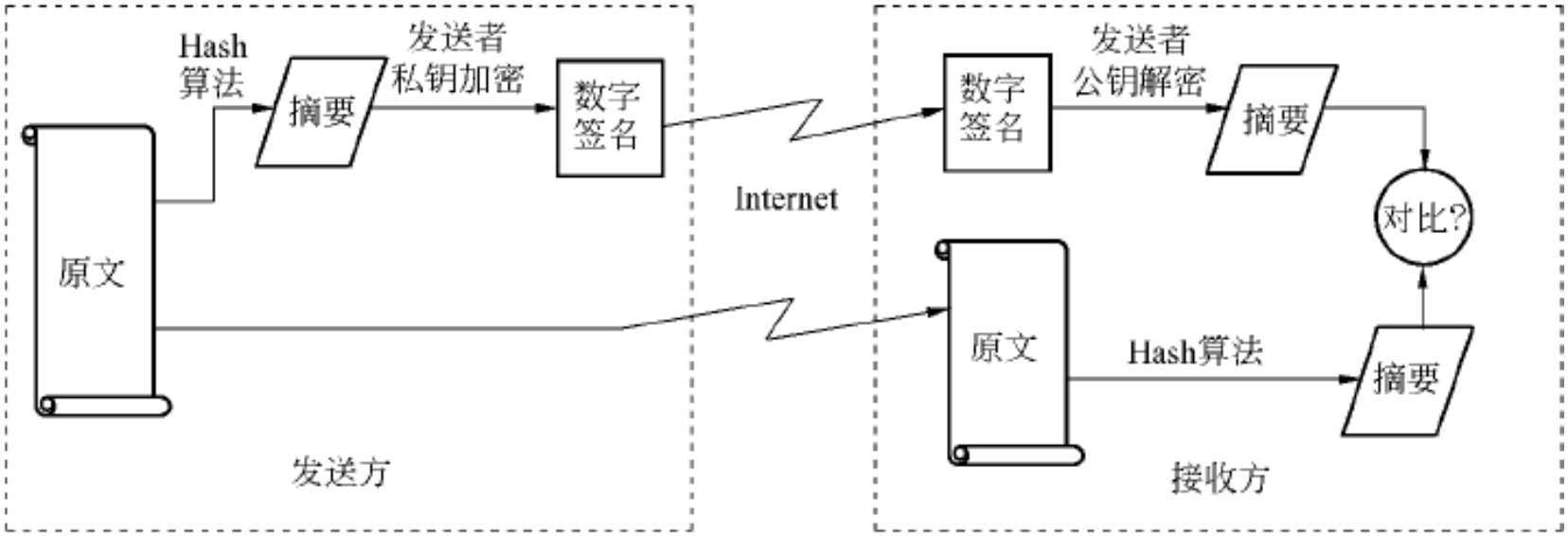
2、数字签名应满足的要求

- 签名是可信的和可验证的，任何人都可以验证签名的有效性。
- 签名是不可伪造的，除了合法的签名者之外，任何人伪造其签名是困难的。
- 签名是不可复制的，对一个消息的签名不能通过复制变为另一个消息的签名。
- 签名的消息是不可改变的，经签名的消息不能篡改，一旦签名的消息被篡改，任何人都可以发现消息与签名之间的不一致性。
- 签名是不可抵赖的，签名者事后不能否认自己的签名（可以由第三方或仲裁方来确认双方的信息，以作出仲裁）。
- 签名的产生、识别和证实必须相对简单。
- 签名必须与签名的信息相关，当签名后的数据发生改变时，该签名将成为无效的签名。

第四节 不可否认技术

3、数字签名的应用模式

- 发送方：用发送方的私钥加密，生成签名，并将签名和原文一起发给接收方。
- 接收方：用发送方的公钥解密，验证签名，匹配一致后接受签名和原文。



第五章 电子商务安全

- 第一节 电子商务的安全需求
- 第二节 信息的保密性技术
- 第三节 数据完整性技术
- 第四节 不可否认技术
- **第五节 身份认证技术**

第五节 身份认证技术

1、数字证书

- 数字证书是一种权威性的电子文档，由权威机构——CA证书认证(Certificate Authority)中心签发，包含了公开密钥持有者信息及其公开密钥，还有认证机构的数字签名。
- 数字证书提供了一种互联网上验证身份的方式，在一个电子商务系统中，所有参与活动的实体都必须用证书来表明自己的身份。
- 证书一方面可以用来向系统中的其它实体证明自己的身份，另一方面由于每份证书都携带着证书持有者的公钥，所以也可以向接收者证实某人或某个机构对公开密钥的拥有，同时也起着公钥分发的作用。

第五节 身份认证技术

1、数字证书

- 简单地说，证书的构成就是一个公钥，再加上公钥所有者的标识，以及被信任的第三方对上述信息的数字签名。公证方的数字签名保证了公钥及其所有者的对应关系，同时也保证了证书中的公钥信息不会被篡改。
- 数字证书类型
  - 按用途分：个人数字证书、服务器数字证书、代码签名证书。
  - 按格式分：X.509、 PGP、 SDSI/SPKI、 X9.59(AADS)、AC等类型的证书。
  - 按协议分：SSL证书（服务于银行对企业或企业对企业的电子商务活动）、SET证书(信用卡消费、网上购物)。

第五节 身份认证技术

1、数字证书

- 数字证书申请和颁发的过程
  - 用户向注册中心RA提出申请：首先在认证中心网站上下载并安装认证中心的根证书；然后填写相关的申请表格，提交相关材料，提出申请。
  - 注册中心首先为用户产生密钥对，然后生成一个称为csr（数字证书请求）的文件，内含公钥及部分用户身份信息。
  - 认证中心CA收到RA的csr文件后，将执行一些必要的核实步骤，以确信请求是真实的，然后进行签名，生成数字证书。该证书内包含有用户的个人信息和他的公钥信息，同时还附有认证中心的签名信息。
  - 用户得到此证书后就可以进行譬如对电子邮件加密等操作。

第五节 身份认证技术

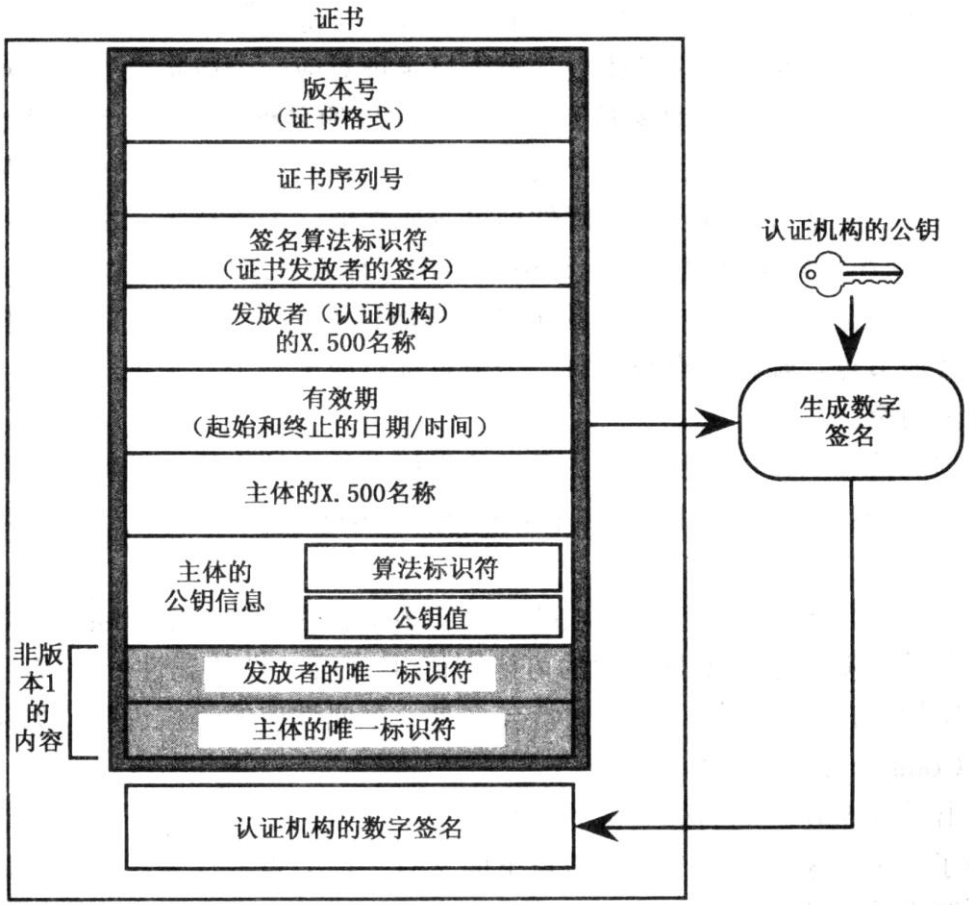
1、数字证书

- 认证中心CA作为电子交易中受信任的第三方，负责为电子商务环境中各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理证书 。
- CA认证中心的四大功能为：证书发放、证书更新、证书撤销和证书验证。具体为：
  - 接收验证用户数字证书的申请。
  - 确定是否接受用户数字证书的申请，即证书的审批。
  - 向申请者颁发（或拒绝颁发）数字证书。
  - 接收、处理用户的数字证书更新请求。
  - 接收用户数字证书的查询、撤销。
  - 产生和发布证书的有效期。
  - 数字证书的归档。
  - 密钥归档。
  - 历史数据归档。

第五节 身份认证技术

1、数字证书

基本数字证书格式



第五节 身份认证技术

2、SSL协议

- SSL协议是一种传输层技术，可以实现兼容浏览器和服务器之间的安全通信。SSL协议是目前网上购物网站中常使用的一种安全协议。
- 所谓SSL就是在和另一方通信前先讲好的一套方法，这个方法能够在它们之间建立一个电子商务的安全性秘密信道，确保电子商务的安全性，凡是不希望被别人看到的机密数据，都可通过这个秘密信道传送给对方，即使通过公共线路传输，也不必担心别人的偷窥。
- 大多数Internet服务器和Web站点都用SSL保证信息交换的安全性。

第五节 身份认证技术

2、SSL协议

- SSL在建立连接过程中采用非对称密钥，在会话过程中使用对称密钥，加密的类型和强度则在两端建立连接的过程中判断决定。
- SSL协议在应用层协议通信之前就完成了加密算法、通信密钥协商以及服务器认证（客户端认证为可选项）工作。在此之后，应用层协议所传输的数据都会被加密，从而保证通信的机密性。
- 建立了SSL安全通道后，只有SSL允许的客户才能与SSL允许的Web站点进行通信，并且在使用URL资源定位器时，输入https:// ，而不是http://。

第五节 身份认证技术

2、SSL协议

缺点：

- SSL协议运行的基点是商家对客户信息保密的承诺。但在上述流程中，SSL协议有利于商家而不利于客户。客户的信息首先传到商家，商家阅读后再传至银行，这样，客户资料的安全性受到威胁。
- 商家认证客户是必要的，但整个过程中，缺少了客户对商家的认证。在电子商务的开始阶段，由于参与电子商务的公司大都是一些大公司，信誉较高，这个问题没有引起人们的重视。随着电子商务参与的厂商迅速增加，对厂商的认证问题越来越突出，SSL协议的缺点完全暴露出来。

第五节 身份认证技术

3、SET协议

- 为了克服SSL安全协议的缺点，满足电子交易持续不断地增加的安全要求，VISA国际组织及其它公司如Master Card、Micro Soft、IBM等共同制定了安全电子交易协议(Secure Electronic Transaction, SET)。
- SET是为在线交易而设立的一个开放的、以电子货币为基础的电子付款系统规范，采用公钥密码体制和X.509数字证书标准，主要应用于B2C模式中保障支付信息的安全性。
- SET在保留对客户信用卡认证的前提下，又增加了对商家身份的认证 （双重签名）。
- SET协议比SSL协议复杂。

第五节 身份认证技术

3、SET协议

SET协议要达到的目标

- 保证电子商务参与者信息的相互隔离。客户的资料加密后通过商家到达银行，但是商家不能看到客户的账户和密码信息。
- 保证信息在因特网上安全传输，防止数据被黑客或被内部人员窃取。
- 解决多方认证问题，不仅要对消费者的信用卡认证，而且要对在线商店的信誉程度认证，同时还有消费者、在线商店与银行间的认证。
- 保证了网上交易的实时性，使所有的支付过程都是在线的。
- 规范协议和消息格式，促使不同厂家开发的软件具有兼容性和互操作功能，并且可以运行在不同的硬件和操作系统平台上。

第五节 身份认证技术

3、SET协议

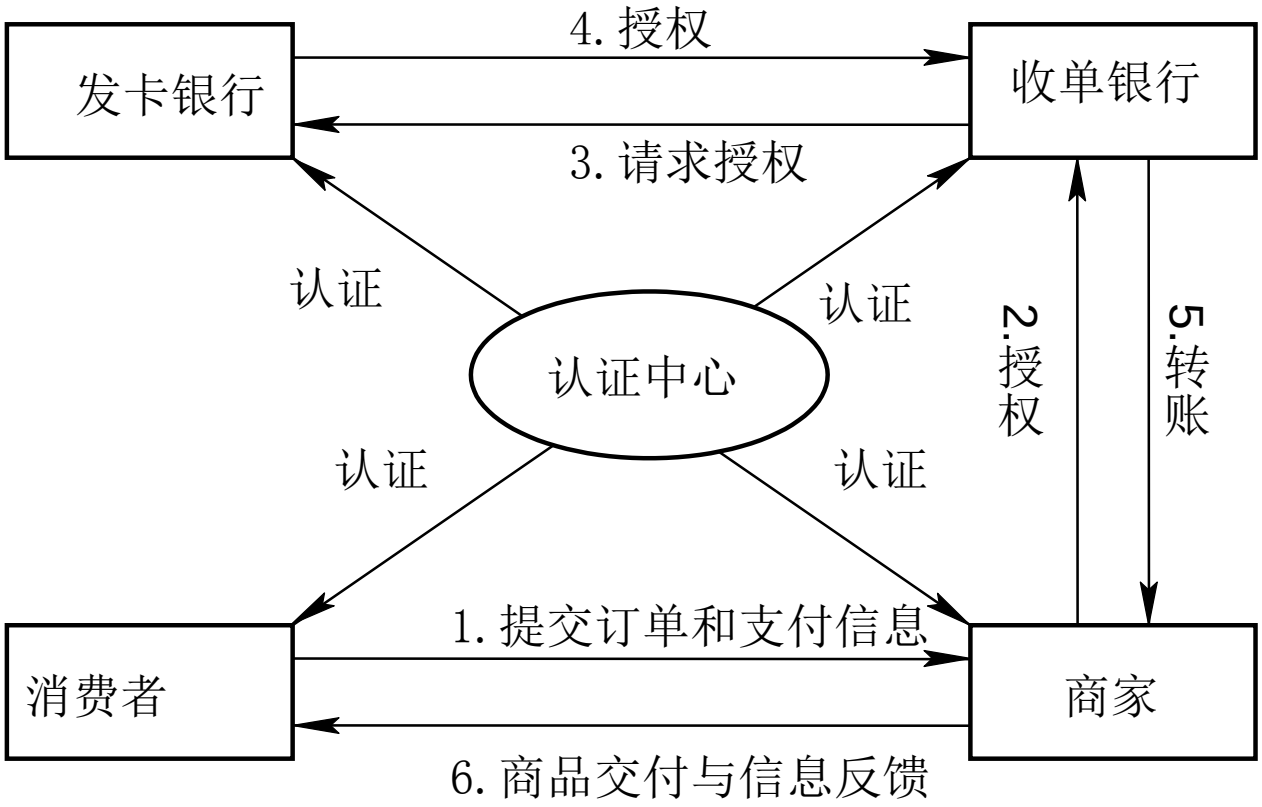
SET的交易成员

- 持卡人：持信用卡购买商品的人，包括个人消费者和团体消费者，按照网上商店的表单填写，通过由发卡银行发行的信用卡进行付费。
- 网上商家：在网上的符合SET规格的电子商店，提供商品或服务，它必须是具备相应电子货币使用的条件，从事商业交易的公司组织。
- 收单银行：通过支付网关处理持卡人和商店之间的交易付款问题事务。接受来自商店端送来的交易付款数据，向发卡银行验证无误后，取得信用卡付款授权以供商店清算。
- 支付网关：这是由支付者或指定的第三方完成的功能。为了实现授权或支付功能，支付网关将SET和现有的银行卡支付的网络系统作为接口。
- 发卡银行：在交易过程开始前，发卡银行负责查验持卡人的数据，若查验有效，整个交易才能成立。在交易过程中负责处理电子货币的审核和支付工作。
- 认证中心CA：可信赖、公正的组织，接受持卡人、商店、银行以及支付网关的数字认证申请书，并管理数字证书的相关事宜。

第五节 身份认证技术

3、SET协议

- 支付流程



第五节 身份认证技术

3、SET协议

- SET安全协议的工作流程主要包括以下7个步骤：
  - 消费者利用已有的计算机通过因特网选定物品，并下电子订单；
  - 通过电子商务服务器与网上商场联系，网上商场做出应答，告诉消费者的订单的相关情况；
  - 消费者选择付款方式，确认订单，签发付款指令(此时SET介入)；
  - 在SET中，消费者必须对定单和付款指令进行数字签名，同时利用双重签名技术保证商家看不到消费者的账号信息；
  - 在线商店接受定单后，向消费者所在银行请求支付认可，信息通过支付网关到收单银行，再到电子货币发行公司确认，批准交易后，返回确认信息给在线商店；
  - 在线商店发送定单确认信息给消费者，消费者端软件可记录交易日志，以备将来查询；
  - 在线商店发送货物或提供服务，并通知收单银行将钱从消费者的账号转移到商店账号，或通知发卡银行请求支付。

第五节 身份认证技术

3、SET协议

SET与SSL比较

- 在认证要求方面，SSL没有SET的安全高，所有参与SET交易的成员都必须申请数字证书进行身份识别。
- 在安全性方面，SET协议规范了整个商务活动的流程，而SSL只对持卡人与商店端的信息交换进行加密保护，可以看作是用于传输的那部分的技术规范。
- 在网络层协议位置方面，SSL是基于传输层的通用安全协议，而SET位于应用层，对网络其他各层也有涉及。
- 在应用领域方面，SSL主要是和Web应用一起工作，而SET是向基于信用卡进行电子化交易的应用提供安全措施的规则。

本章小结

- 电子商务的安全需求和基本特性
- 信息的保密技术：加密/解密与防火墙
- 数据完整性技术及不可否认技术：消息摘要/数字签名
- 身份认证技术（CA认证）：数字证书和认证中心

Thank You !