



信息安全导论

第三讲 数字签名与身份认证





第三讲 签名与认证基础知识 > 主要内容

1

安全协议

2

数字签名

3

消息认证与身份认证





安全协议

安全协议，是以密码学为基础的消息交换协议，此定义包含以下两层含义：

- (1) 安全协议以**密码学为基础**；体现了安全协议与普通协议之间的差异。
- (2) 安全协议也是**通信协议**。





第三讲 签名与认证基础知识 > 安全协议中的角色

参与者

协议执行的双方或是多方,也就是人们常说的发送方和接收方。

- (1) 可能是完全信任的人
- (2) 也可能是攻击者或是完全不信任的人

比如:

- 认证协议的发起者和响应者,
- 证明中的证明人和验证者,
- 电子商务中的商家、银行、和客户等.





攻击者

攻击者就是协议过程中企图破坏协议**安全性**和**正确性**的人。

(1) 不影响协议执行的攻击者称为**被动攻击者**，他们仅仅观察协议并试图获取信息

(2) 还有一类攻击者叫做**主动攻击者**，他们改变协议，在协议中引入新消息，修改消息或删除消息等，达到欺骗，获取敏感信息，破坏协议等目的等。





可信第三方

可信第三方(Trusted Third Party)是指在完成协议过程中, 值得信任的第三方, 能帮助互不信任的双方完成协议。**仲裁者**是一类特殊的第三方,用来解决协议执行过程中出现的纠纷。仲裁者是在完成协议的过程中, **值得信任的公正的**第三方。

(1) “公正”意味着仲裁者在协议中无有既得利益, 与参与协议的任何人也没有特别的利害关系。

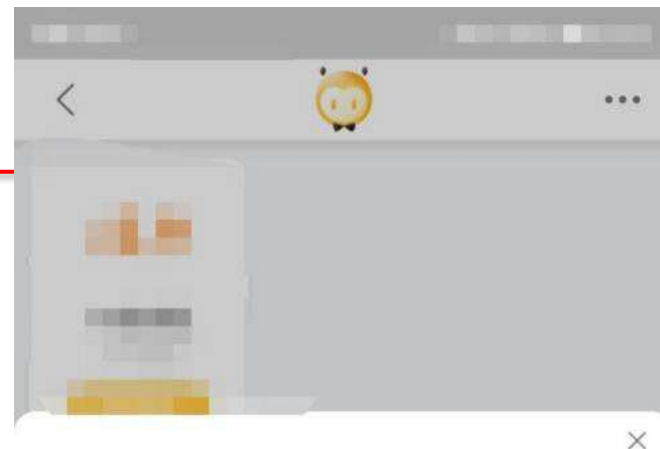
(2) “值得信任”表示协议中的所有人都接受仲裁结果,即仲裁者说的都是真实的, 它做的仲裁是正确的, 并且他将完成协议中涉及的其他部分。其他可信第三方如密钥分发中心, 认证中心等。





- 生活中的可信第三方：

- 淘宝 小二
- 法院
- ...



点击【淘宝介入】后，会给予 **3天的举证期**，如果需要买家举证的，还会给予 **卖家24小时的处理期**，之后会进入到淘宝审核凭证期，将会 **在48小时内核实处理**，请您耐心等待淘宝的处理结果。

您可能还想了解：

- [如何申请淘宝客服介入？](#)
- 交易纠纷处理依据《争议处理规范》，请[点此查看](#)。

温馨提示：

- 您申请客服介入后维权小二会在48小时内介入核实，您也可登录【我的淘宝】-【我的订单-【退款管理】或【我的淘宝】-【退款/售后】找到您已经申请退款的订单，查看退款状态及处理结果。
- 在您点击要求淘宝客服介入处理并完成举证后，维权小二会在48小时内介入处理，目前无法支持提前介入的诉求，还请您耐心等待哦！





安全协议

最常用的安全协议主要有以下四类：

- 1、**密钥生成协议**
- 2、**认证协议**
- 3、**电子商务协议**
- 4、**安全多方计算协议**





密钥建立协议

- 在网络通信中, 通常使用对称密码算法用单独的密钥对每一次单独的会话加密, 这个密钥成为会话密钥.
- 密钥建立协议的**目的**是在两个或是多个实体之间建立共享的会话密钥.
- 可以采用对称密码体制或者非对称密码体制建立会话密钥.
 - 有时借助一个可信的服务器为用户分发密钥, 这样的密钥建立协议成为**密钥分发协议**;
 - 也可以通过两个用户协商, 共同建立会话密钥, 这样的密钥建立协议称为**密钥协商协议**.





认证协议

- 认证是对数据, 实体标识的保证.
- **数据起源认证**能够提供数据的完整性, 因为非授权的改变意味着数据来源的改变.
- **实体认证**是确认某个实体是它所声称的实体的过程, 可能涉及证实用户的身份.
- 认证协议主要目的防止假冒攻击.
- 将**认证和密钥建立协议**结合在一起, 是网络通信中最普遍应用的安全协议.





电子商务协议

- 电子商务就是利用各种电子信息进行商务活动.
- 电子商务的主体往往代表交易的双方, 其利益目标不一致. 因此, 电子商务协议最关注公平性, 即协议应保证交易双方都不能通过损害对方的利益而获取其不应该得到的利益.
- 常见的电子商务协议有电子现金协议, 电子选举协议, 拍卖协议, SET协议等.





安全多方计算协议

- 安全多方计算协议的目的是保证分布式环境中参与方以安全的方式执行分布式计算任务. 考虑到分布式计算的环境, 总假定协议在执行过程中会受到一个来自外部的实体, 甚至来自内部的一组参与方的攻击. 这种假设很好的反应了网络环境下的安全需求.
- 安全多方计算协议的两个基本的安全要求就是保证协议的正确性和各参与方私有输入的秘密性, 即协议执行完之后参与各方都能够得到正确的结果, 并且除此之外不能获知其他任何信息.
- 安全多方计算协议包括抛币协议, 广播协议, 选举协议, 电子竞标和拍卖协议, 电子现金协议合同签署协议, 匿名交易协议, 保密信息检索, 保密数据库访问, 联合签名, 联合解密等协议.





安全多方计算协议：百万富翁问题

- 两个富翁，分别为Alice和Bob。他们自己都清楚自己有几百万财产，也即，他们心里清楚 1~10中的一个数（代表自己百万级的财富）；他们想知道到底谁的数更大一些。
- 这里假定：
 - 两人都值得信任，不会作假
 - 两人都希望诚实地比较出谁更服务（即谁的数更大）
 - 两人又都希望知道对方财产到底是多少，如果可能的话，拿到具体数字最好了
 - 其实这里假定的是一个安全多方计算的模型 - 半诚实对手模型，即计算方存在获取其他计算方原始数据的需求，但仍然按照计算协议执行。





安全多方计算协议：百万富翁问题

- 一个简单的解决方案就是一下步骤：
 1. Alice找10个一模一样的箱子，按照1 ~ 10的顺序摆好，并按照自己的财富值分别往里面放入苹果梨和香蕉，具体放法为：如果序号小于自己的财富之，放入苹果，相等，则放入梨，大于自己的财富值，放入香蕉；把10个盒子都叫上锁；
 2. 并叫Bob过来（或者寄给Bob）Bob根据自己的财富值对相应的箱子再加一把锁。然后把其他所有箱子销毁。并把这个选择的箱子送给Alice。

YAO A C. Protocols for secure computation[C]. In Proc. of the 23rd Annual Symposium on Foundations of Computer Science, 1982.





安全多方计算协议：百万富翁问题

- 一个简单的解决方案就是一下步骤：
- Alice看到送回来的箱子，但他不知道Bob选择的是第几个箱子，因为每个箱子都是一样的。
- Alice、Bob分别开锁，看里面是什么水果：
 - 如果是苹果，Alice比Bob富有；
 - 如果是梨，两人一样有钱；
 - 如果是香蕉，Bob比Alice富有；
- 简单吧，可行吗？当然可行！前提是双方都是可信的，双方会遵守协议，所以这是一个半诚实对手模型。如果有一方造假，那么结果就不可信了。那是恶意敌手模型要讨论的问题。





第三讲 签名与认证基础知识 > 数字签名

数字签名

数字签名技术是实现交易安全的核心技术之一，它的实现基础就是加密技术。

美国发布数字签名标准

DSS(Digital Signature Standard), 1991

《中华人民共和国电子签名法》(2004年)

数据电文中以电子方式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

应用：身份认证、不可否认性





双方之间不可以用消息验证来替代数字签名，数据交换有两种欺骗：

- 1) Bob 伪造一个消息并使用与 Alice 共享密钥 K 产生该消息认证码，然后声称消息来自 Alice（实际 A 未产生过任何消息）**
- 2) Alice 可以对自己产生的消息予以否认，因为 Bob 也可以产生。**





数字签名必须具有以下特点

- ①发送方必须用自己独有的信息来签名以防止（别人）伪造和（自己）否认
- ②签名很容易产生
- ③接收方很容易验证签名的真伪（所以如RSA公钥很短，速度快）
- ④对于给定的 x ，找出 y ($y \neq x$) 使得签名 $S(y) = S(x)$ 在计算上是不可行的
- ⑤找出任意两个不同的输入 x 、 y ，使得 $S(y) = S(x)$ 在计算上是不可行的

数字签名一般有两部分组成：

签名算法（私钥秘密保存）

验证算法（公钥公开）





数字签名必须保证：

- ❖可验证： 签字是可以被确认的**
- ❖防抵赖： 发送者事后不承认发送报文并签名；**
- ❖防假冒： 攻击者冒充发送者向收方发送文件；**
- ❖防篡改： 收方对收到的文件进行篡改；**
- ❖防伪造： 收方伪造对报文的签名。**

签名对安全、防伪、速度要求比加密更高。





数字签名分类

·以方式分

①直接数字签名direct digital signature

②仲裁数字签名arbitrated digital signature

常见的数字签名算法有RSA, DSA, Rabin, ElGamal, Schnoor, OSS, ESI GN等。

现在普遍使用的数字签名算法，大都是基于以下三个数学难题的基础上的：

- ◆整数因子分解问题，如RSA算法。
- ◆离散对数问题，如ElGamal, DSA, Schnoor等算法。
- ◆椭圆曲线离散对数问题，如ECDSA算法。





① 参数

p: 满足 $2^{L-1} < p < 2^L$ 的大素数，其中 $512 \leq L \leq 1024$ 且L是64的倍数.

q: p-1的素因子，满足 $2^{159} < q < 2^{160}$ ，即q长为160比特.

g: $g \equiv h^{(p-1)/q} \pmod p$ ，其中h是满足 $1 < h < p-1$ 且使得 $h^{(p-1)/q} \pmod p > 1$ 的任一整数.

用户私钥x ($0 < x < q$ 的随机数或伪随机数) ;

用户的公钥y: $y \equiv g^x \pmod p$.





② 签名过程

➤ 用户为待签消息选取的秘密数 r ， r 是满足 $0 < r < q$ 的随机数(伪随机数)。

➤ 用户对消息 m 的签名为 (s, t)

$$t \equiv (g^r \bmod p) \bmod q,$$

$$s \equiv [r^{-1}(h(m) + xt)] \bmod q,$$

$H(M)$ 是由SHA求出的消息 M 的杂凑值。





③

验证过程

设接收方收到的消息为 M 及其签名 (s', t') ,
计算

$$w \equiv (s')^{-1} \bmod q, u_1 \equiv [h(M)w] \bmod q$$

$$u_2 \equiv t'w \bmod q, v \equiv [(g^{u_1}y^{u_2}) \bmod p] \bmod q$$

检查若 $v=t$ 相等, 则认为签名有效.





RSA数字签名

签名方利用RSA算法产生公钥 (n, e) 和私钥 d .

签名过程:

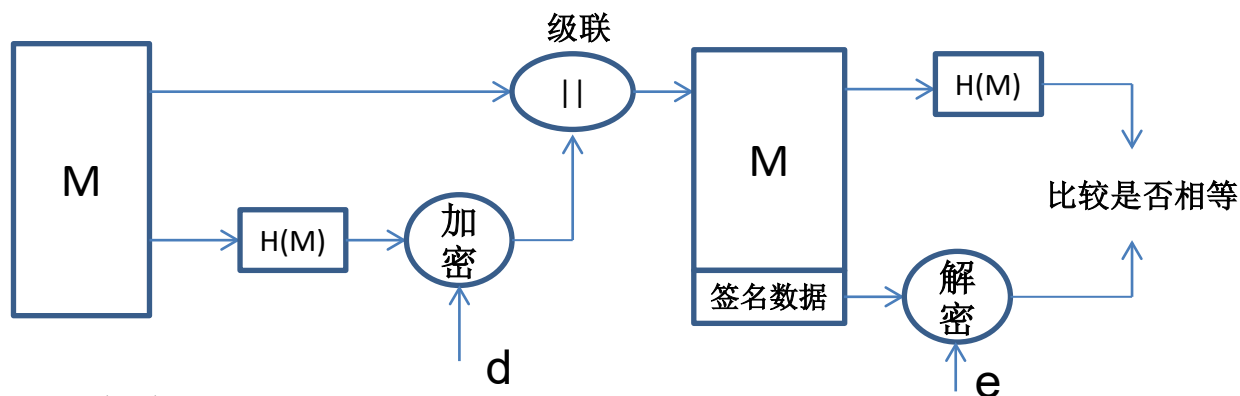
- (1) 首先利用摘要算法计算消息的摘要 $H(M)$;
- (2) 用私钥 d 加密消息摘要得到签名信息:

$$s = H(M)^d \bmod n;$$

发送 (M, S)

验证过程:

- (1) 用同样方法计算消息摘要 $H(M)$;
- (2) 用公钥 (n, e) 解密签名信息得到: $H(M)$,
如果 $H(M) = H(M)$, 那么就接受该签名。





多重数字签名

需要两个或多个人员同时对一份文件进行签名，例如共同签署协议的Alice、Bob、Carlos甚至更多人员。三种签名方案：

1. Alice和Bob分别对文件的副本签名
2. Alice首先对文件进行签名，然后Bob对Alice的签名再进行签名
3. 利用单向Hash函数实现多重签名（P55最下方，重点）





签名方希望有这样一种数字签名方案：在没有签名方的同意下，接收方不能把签名给第三者看。不可抵赖数字签名正是这样一种方案。

不可抵赖数字签名的思想：

- 1、Alice向Bob出示一个签名。
- 2、Bob产生一个随机数并送给Alice。
- 3、Alice利用随机数和其私人密钥进行计算，并将计算结果发送给Bob。Alice只能计算该签名是否有效。
- 4、Bob确认这个结果。





盲签名

A不想让B指导消息内容，又想让B签名，怎么办？

1) A对消息n做个随机掩盖（如乘以 k^e , e是公钥），然后发给B, 要求B用私钥签名（盲签名）。

A选取随机数k掩盖消息m 计算 $t = m \cdot k^e \mod n$, 发给B;

B用自己私钥d签名掩盖好的t, $t^d = (m \cdot k^e)^d \mod n = m^d \cdot k \mod n$

因为 $k^{ed} = k$, ed互为公私钥 ↗

2) A拿回盲签名，先除以k解掩盖, 就得到了B的签名，这样A可以将该B的签名发给预定方，而B不知道消息内容，A也不知道B的私钥。

A拿回 t^d , 计算 $t^d / k = m^d \mod n$, 即是与B对n的签名





第三讲 签名与认证基础知识 > 消息认证和身份认证

消息认证：对消息的认证；身份认证：对身份的认证

消息认证是使预定的消息接收者能够检验收到的消息是否真实的方法。检验内容应包括：

- ❖ (1) 证实报文的源
- ❖ (2) 报文内容是否曾受到偶然的或有意的篡改
- ❖ (3) 报文的序号和时间栏

即：消息的源，内容的真伪，时间性 （P59第二段）

- ❖ 这种认证只在相应通信的双方之间进行，而不允许第三者进行上述认证。认证不一定是实时的，可用消息认证码MAC对消息做认证。采用Hash函数。





1 单向函数

已知 x 计算 y 使得 $y=f(x)$ 很容易;

但若已知 y 计算 x , 使得 $x=f^{-1}(y)$ 就很困难.

2 Hash函数

把可变长度的输入字符串映射为固定长度的输出字符串, 输出字符串就叫Hash值.

如果不同的输入经过Hash映射后却得到相同的Hash 值, 就说Hash函数产生冲突.

好的Hash函数应该无冲突.

公开





3 单向陷门函数

单向陷门函数满足下面三个条件：

- ❖ 对 $f(n)$ 的定义域中的每一个 n ，均存在函数 $f^{-1}(n)$ ，使得 $f^{-1}(f(n)) = f(f^{-1}(n)) = n$ ；
- ❖ $f(n)$ 与 $f^{-1}(n)$ 都很容易计算；
- ❖ 仅根据已知的计算 $f(n)$ 的算法，去找出计算 $f^{-1}(n)$ 的容易算法是非常困难的。

单向和**hash**：不可逆

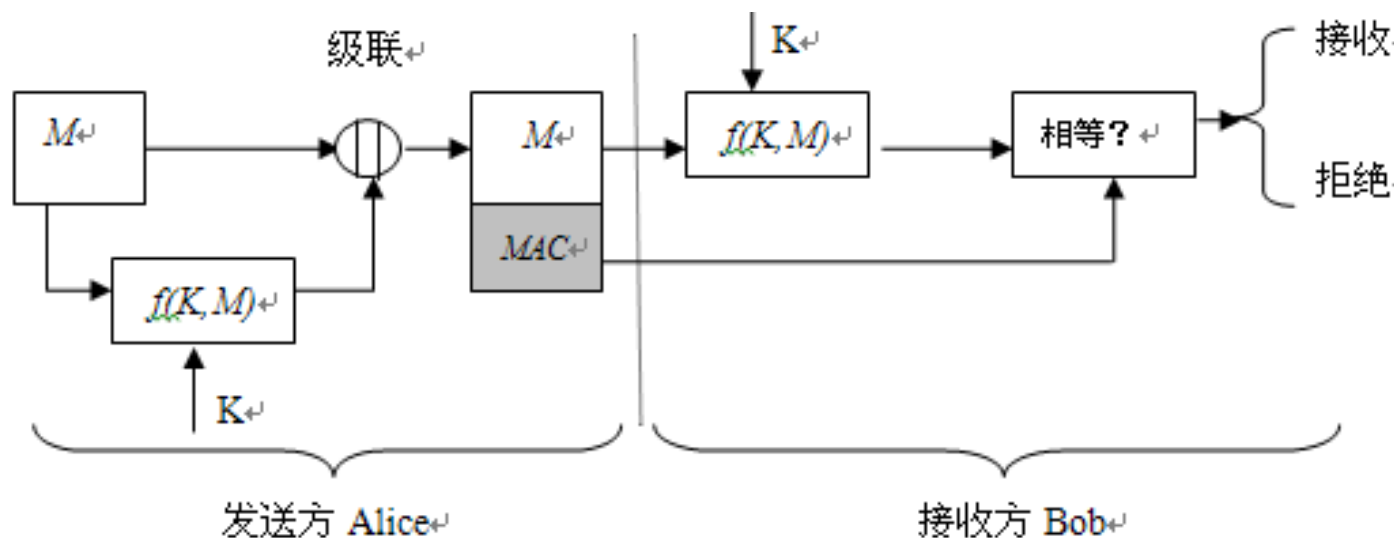
单向陷门：非对称密码学基础，碎纸编号可逆（否则不可能）





消息认证的基本方法有两种，一是采用Hash函数，二是采用消息认证码(Message Authentication Code, MAC)。这两种方法的区别在于是否需要密钥的参与。

认证码被附加到消息后以 $M\parallel MAC$ 方式一并发送，接收方通过重新计算MAC以实现对其认证，如图所示。



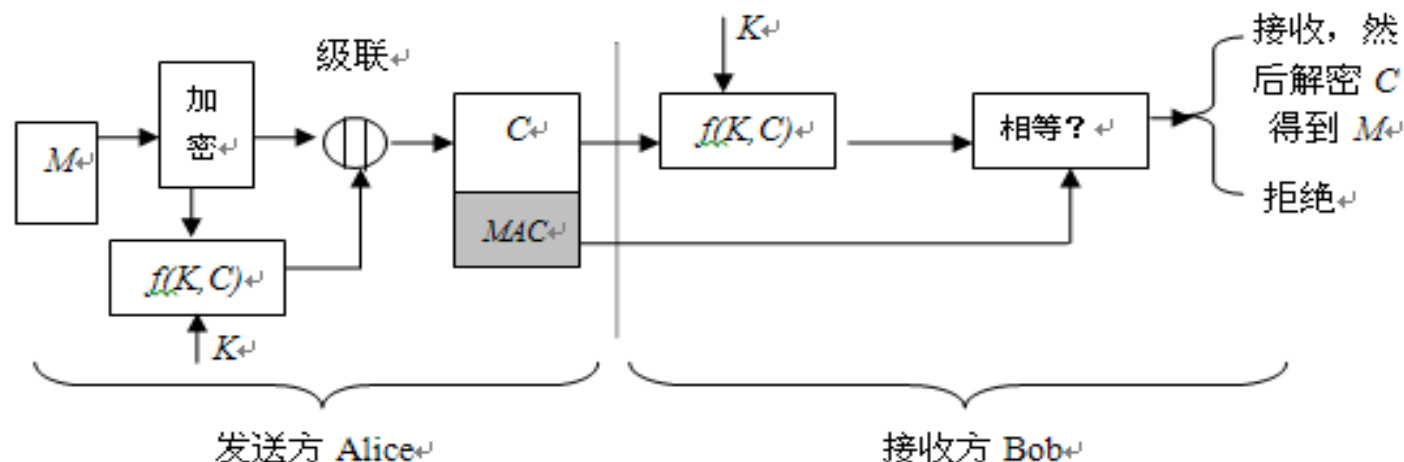
MAC 认证方式示意图

提问：把 $f(K, M)$ 改成Hash (M)，安全吗？

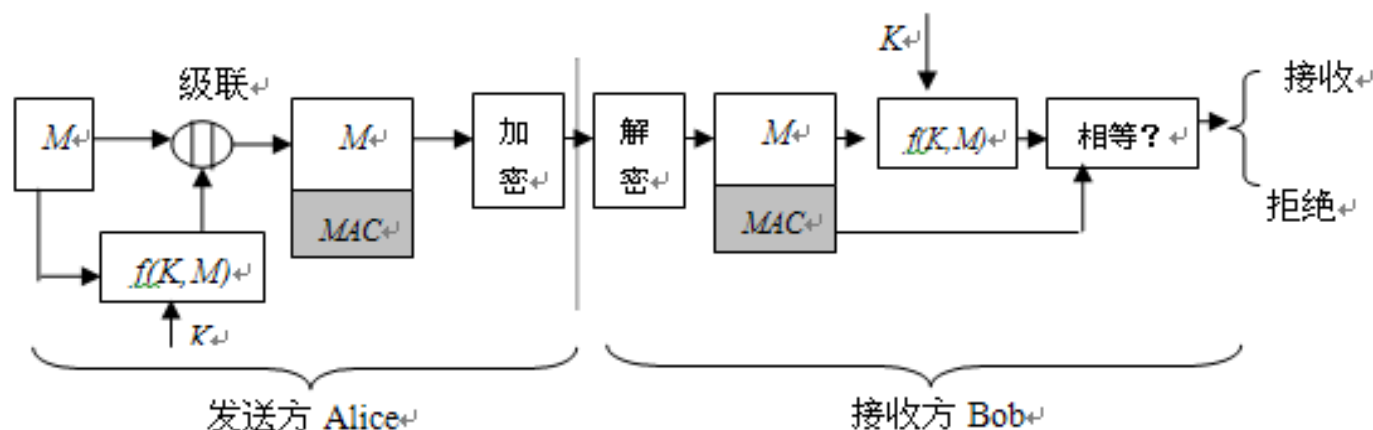




不暴露消息的消息认证



MAC 认证方式示意图——只加密 M



MAC 认证方式示意图——加密整个消息

提问：把 $f(K, M)$ 改成 $\text{Hash}(M)$ ，安全吗？





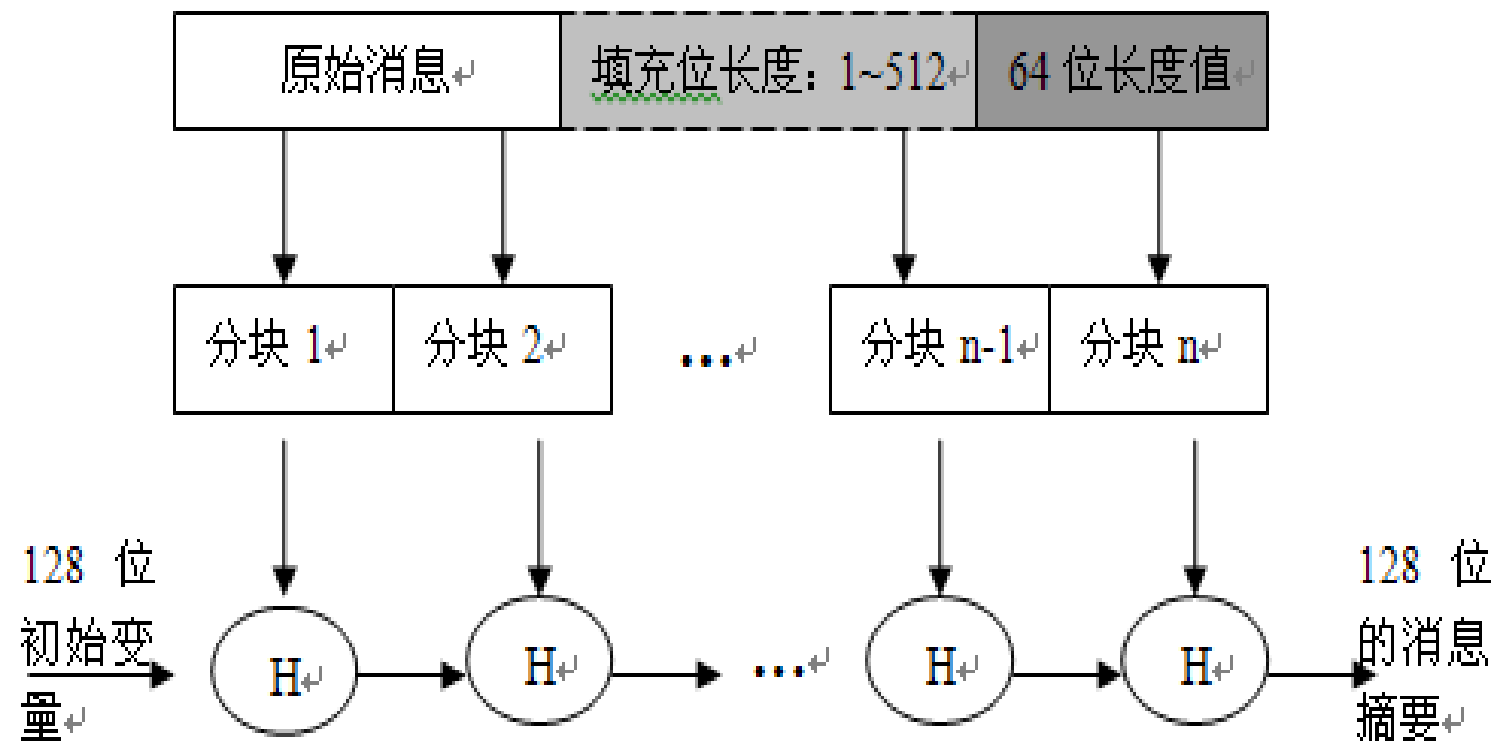
采用HASH的消息认证--把上述三幅图 $f(K, M)$ 变为HASH(M)

消息认证算法

1. MD5算法

MD表示消息摘要(Message Digest, MD)。MD4算法是1990年由Ron Rivest设计的一个消息摘要算法,该算法的设计不依赖于任何密码体制,采用分组方式进行各种逻辑运算而得到。1991年MD4算法又得到了进一步的改进,改进后的算法就是MD5算法。MD5算法以512 bit为一块的方式处理输入的消息文本,每个块又划分为16个32 bit的子块。算法的输出是由4个32 bit的块组成的,将它们级联成一个128 bit的摘要值。MD5算法如图所示,包括以下几个步骤。





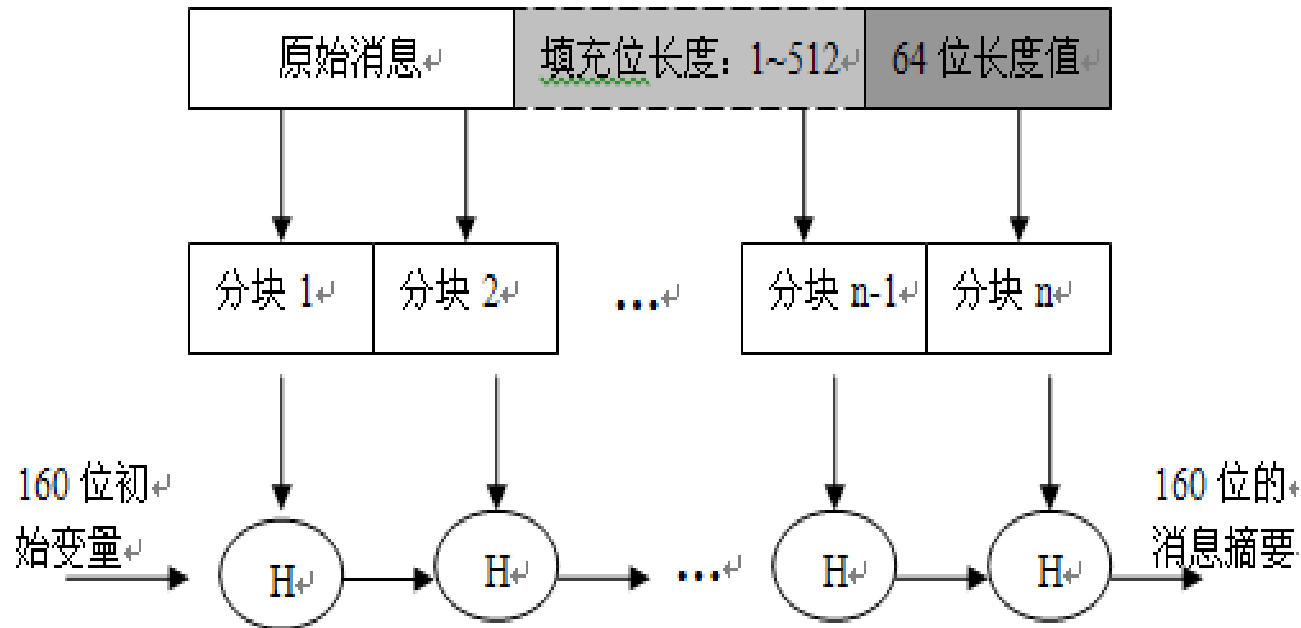
MD5 算法过程示意图





消息认证算法-SHA

SHA (Secure Hash Algorithm, SHA) 由美国NIST开发，作为联邦信息处理标准于1993年发表，1995年修订后，成为SHA1版本。SHA1算法在设计方面基本上是模仿MD5算法，如图所示，包含以下几个过程。



SHA 算法过程示意图



第三讲 签名与认证基础知识>基本概念

什么是身份认证



身份认证是证实主体的真实身份与其所声称的身份是否相符的过程，身份认证可分为**用户与主机**间的认证和**主机与主机**之间的认证。



第三讲 签名与认证基础知识 > 身份认证

★ 理解

身份认证的方法

身份认证的依据应包含只有该用户所特有的、并可以验证的特定信息。

基于口令

方法一、用户所知道的或所掌握的信息如密码、口令等；

what you know

基于智能卡

方法二、用户所拥有的特定东西如身份证、护照、密钥等；

what you have

基于生物特征

用户所具有的个人特征如指纹、笔迹、声纹、虹膜、DNA等。（生物特征的认证技术）

who you are



第三讲 签名与认证基础知识 > 身份认证



身份认证的分类

根据认证条件的数目分类

仅通过一个条件的相符合来证明一个人的身份，称之为单因子认证；通过两种不同条件来证明一个人的身份，称之为双因素认证；通过组合多种不同条件来证明一个人的身份，称之为多因素认证。

根据认证数据的状态来看

静态数据认证：指用于识别用户身份的认证数据事先已产生并保存在特定的存储介质上
动态数据认证：指用于识别用户身份的认证数据不断动态变化，每次认证使用不同的认证数据，即动态密码



第三讲 签名与认证基础知识 > 身份认证


实例一

静态数据认证：静态密码

用户的密码是由用户自己设定的。在网络登录时输入正确的密码，计算机就认为操作者就是合法用户。实际上，由于许多用户为了防止忘记密码，经常采用诸如生日、电话号码等容易被猜测的字符串作为密码，或者把密码抄在纸上放在一个自认为安全的地方，这样很容易造成密码泄漏。如果密码是静态的数据，在验证过程中需要在计算机内存中和传输过程可能会被木马程序或网络中截获。因此，静态密码机制无论是使用还是部署都非常简单，但从安全性上讲，用户名/密码方式一种是不安全的身份认证方式。它利用 **what you know** 方法。

Sign in

Microsoft account [What's this?](#)

@yahoo.com.cn

.....

☐ Keep me signed in

Sign in

[Can't access your account?](#)

[Sign in with a single-use code](#)

Baidu 经验
jingyan.baidu.com

第三讲 签名与认证基础知识 > 身份认证

实例二

静态数据认证：智能卡

一种内置集成电路的芯片，芯片中存有与用户身份相关的数据，智能卡由专门的厂商通过专门的设备生产，是不可复制的硬件。智能卡由合法用户随身携带，登录时必须将智能卡插入专用的读卡器读取其中的信息，以验证用户的身份。

智能卡认证是通过智能卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此还是存在安全隐患。它利用 **what you have** 方法。



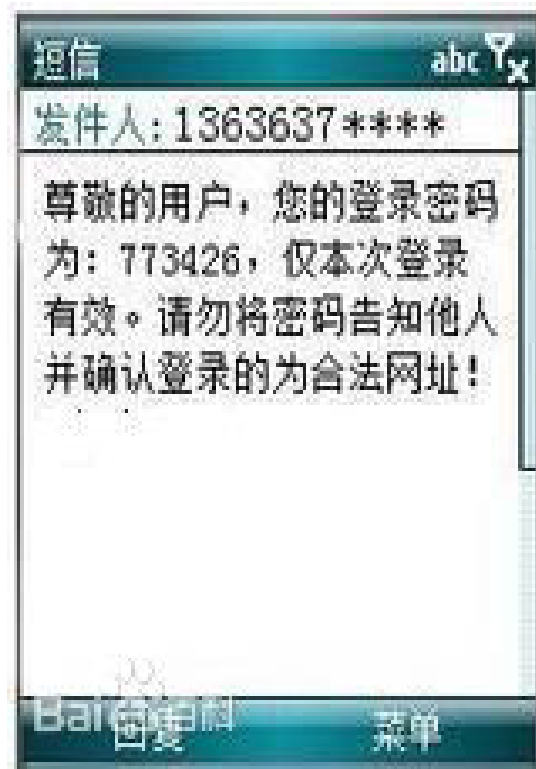


第三讲 签名与认证基础知识 > 身份认证

实例三

动态数据认证：短信密码

短信密码以手机短信等形式请求包含6位随机数的动态密码，身份认证系统以短信形式发送随机的6位密码到客户的手机上。客户在登录或者交易认证时候输入此动态密码，从而确保系统身份认证的安全性。它利用 **what you have** 方法。



第三讲 签名与认证基础知识>身份认证

实例四

动态数据认证：动态口令卡

动态口令牌是客户手持用来生成动态密码的终端，主流的是基于时间同步方式的，每60秒变换一次动态口令，口令一次有效，它产生6位动态数字进行一次一密的方式认证。

目前最为安全的身份认证方式之一，也利用what you have方法。



第三讲 签名与认证基础知识 > 身份认证

实例五

静态数据认证：生物特征认证

运用who you are方法，通过可测量的身体或行为等生物特征进行身份认证的一种技术。生物特征分为身体特征和行为特征两类。身体特征包括：指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和DNA等；行为特征包括：签名、语音、行走步态等。应用广泛的领域有门禁系统等。



第三讲 签名与认证基础知识 > 身份认证

实例六

双因子认证：USBKEY

基于USB Key的身份认证方式是近几年发展起来的一种方便、安全的身份认证技术。它采用软硬件相结合的**强双因子**认证模式，很好地解决了安全性与易用性之间的矛盾。

USB Key是一种USB接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用USBKey内置的密码算法实现对用户身份的认证。使用USBKEY通常需要提供个人认证信息。





第三讲 签名与认证基础知识 > 身份认证

认证协议

实现认证必须要求示证方和验证方遵循一个特定的规则来实施认证，这个规则被称为认证协议



记忆

参与协议的主体

一方是出示证件的人，称作**示证者P** (Prover)，又称声称者 (Claimant)；

另一方为**验证者V** (Verifier)，检验声称者提出的证件的正确性和合法性，决定是否满足要求；

可信第三方TTP (Trusted third party)，参与调解纠纷；

第四方是**攻击者** (adversary)，可以窃听或伪装声称者骗取验证者的信任





Dolev—Yao 模型

攻击者模型

对攻击者知识和能力的描述

★ 记忆

Dolev和Yao认为攻击者具有如下能力：（Dolev-Yao模型）

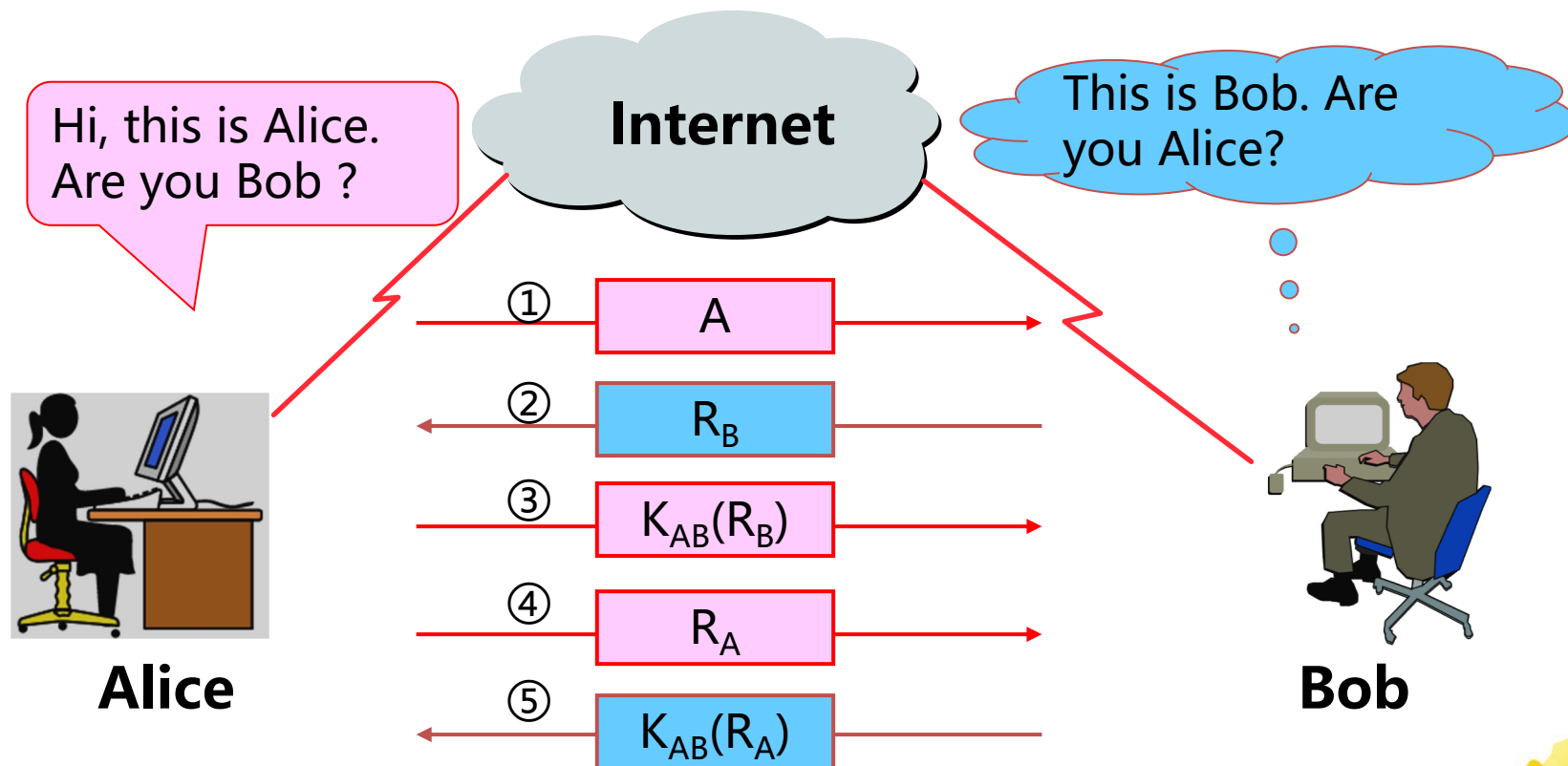
- (1) 可以窃听所有经过网络的消息；
- (2) 可以阻止和截获所有经过网络的消息；
- (3) 可以存储所获得或自身创造的消息；
- (4) 可以根据存储的消息伪造消息，并发送该消息；
- (5) 可以作为合法的主体参与协议的运行。



第三讲 签名与认证基础知识 > 身份认证

基于对称密钥体制的认证协议

在这种协议中，鉴别双方共享一个对称密钥 K_{AB} ，该对称密钥在鉴别之前已经协商好（不通过网络）。

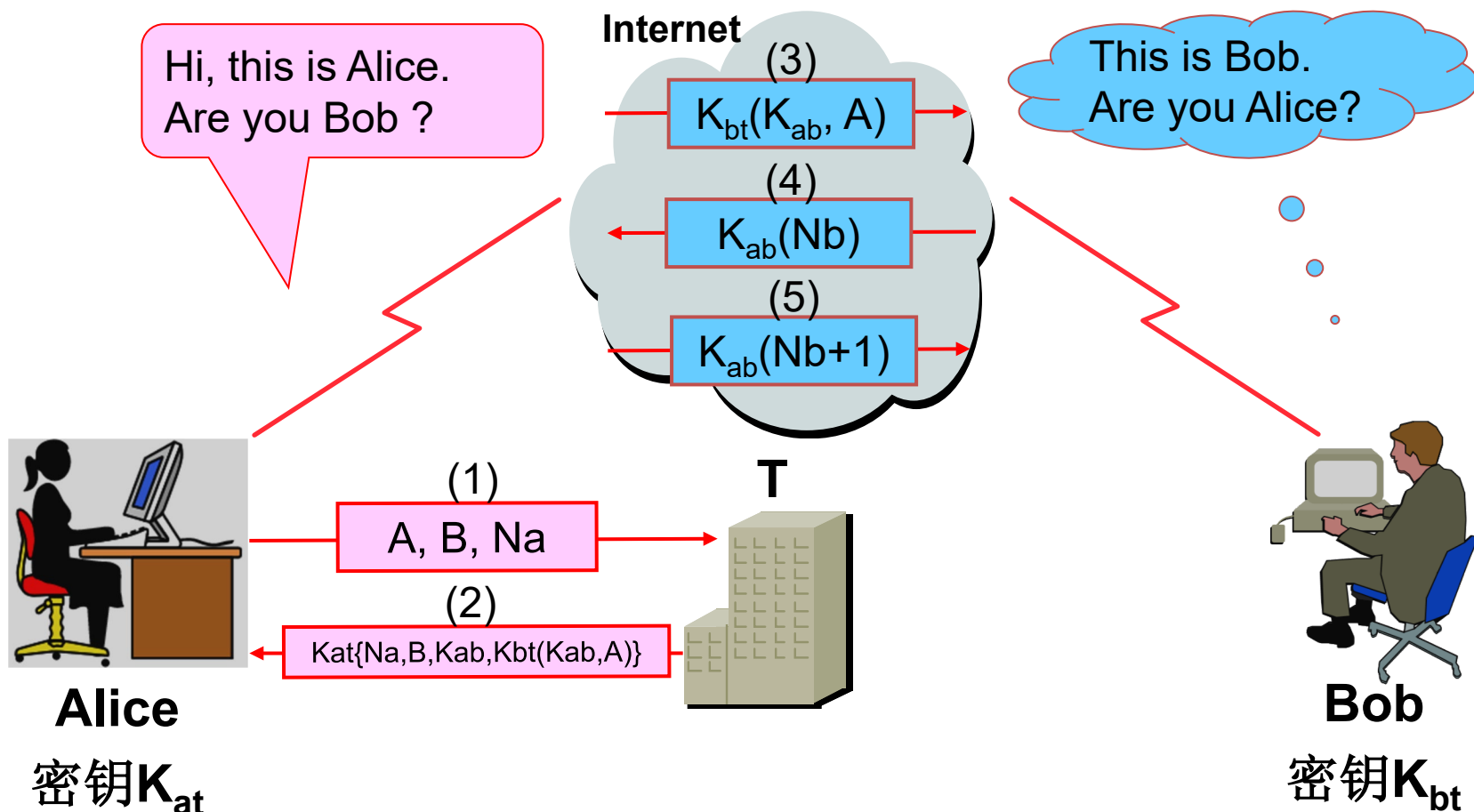


第三讲 签名与认证基础知识 > 身份认证

重点掌握 P70

基于NS协议的身份认证协议

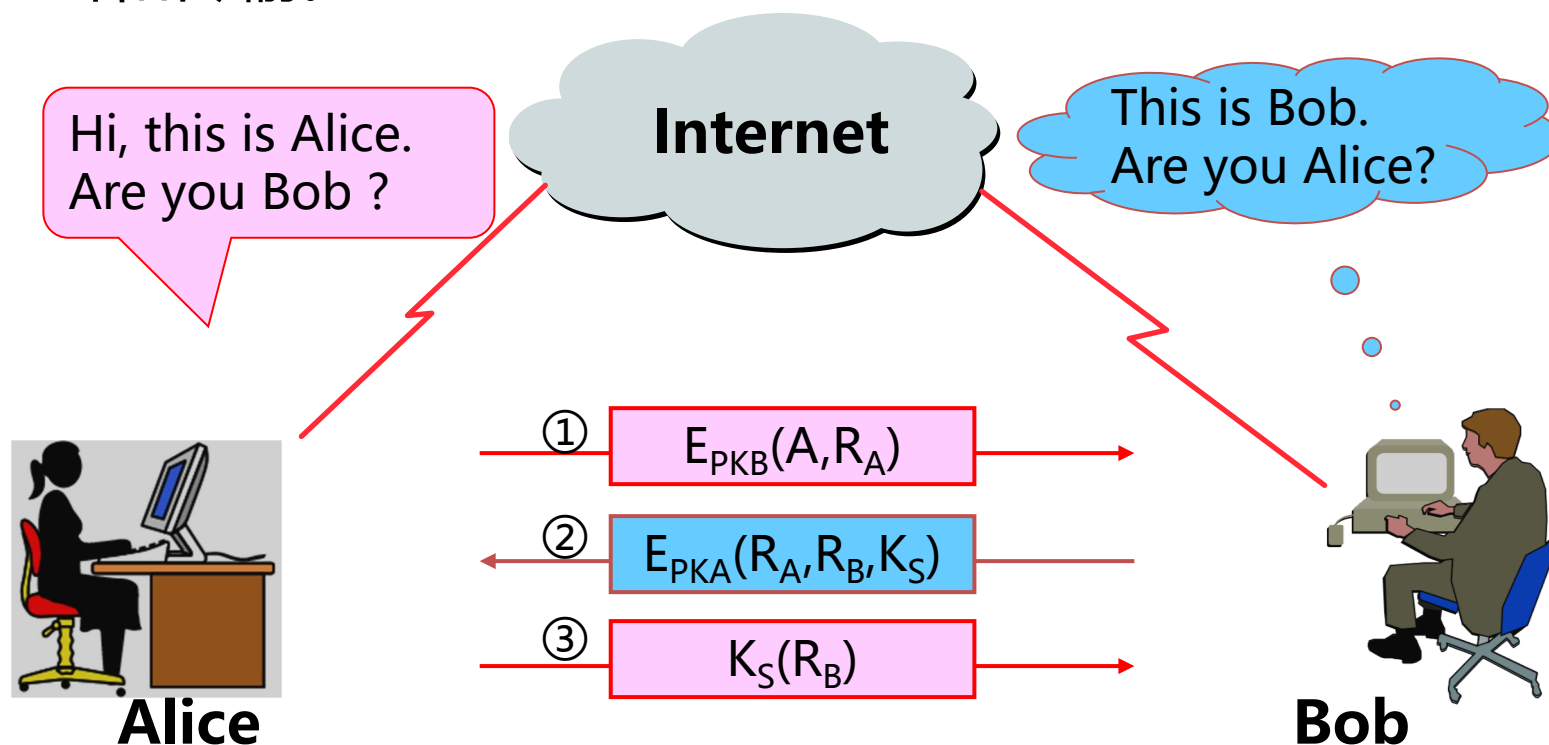
由Needham和Schroeder于1978年提出，包括对称和非对称版本。
NS协议的对称密码版本主体有三个：通信双方A、B，以及可信第三方T。



第三讲 签名与认证基础知识 > 身份认证

基于非对称密钥体制的身份认证协议

在这种认证协议中，双方均用对方的公开密钥进行加密和传输。

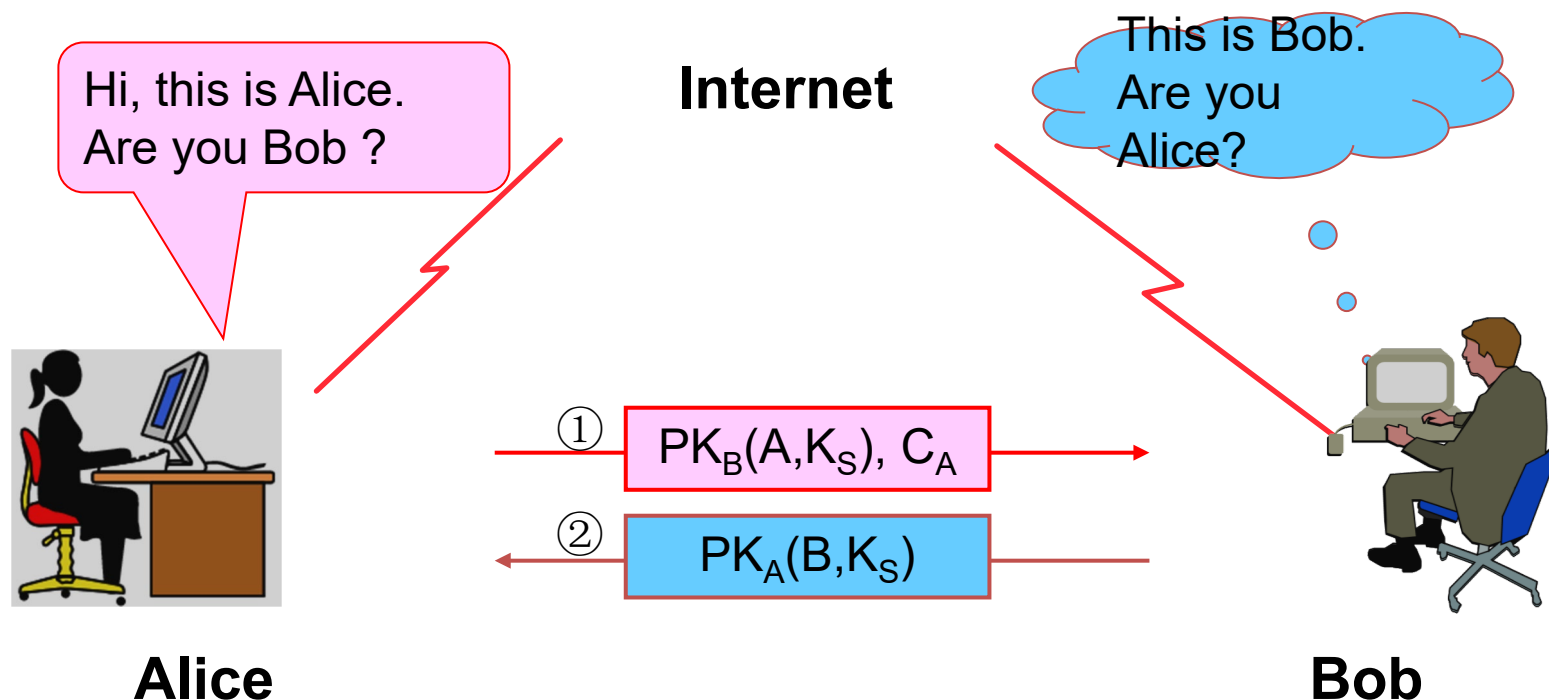




第三讲 签名与认证基础知识 > 身份认证

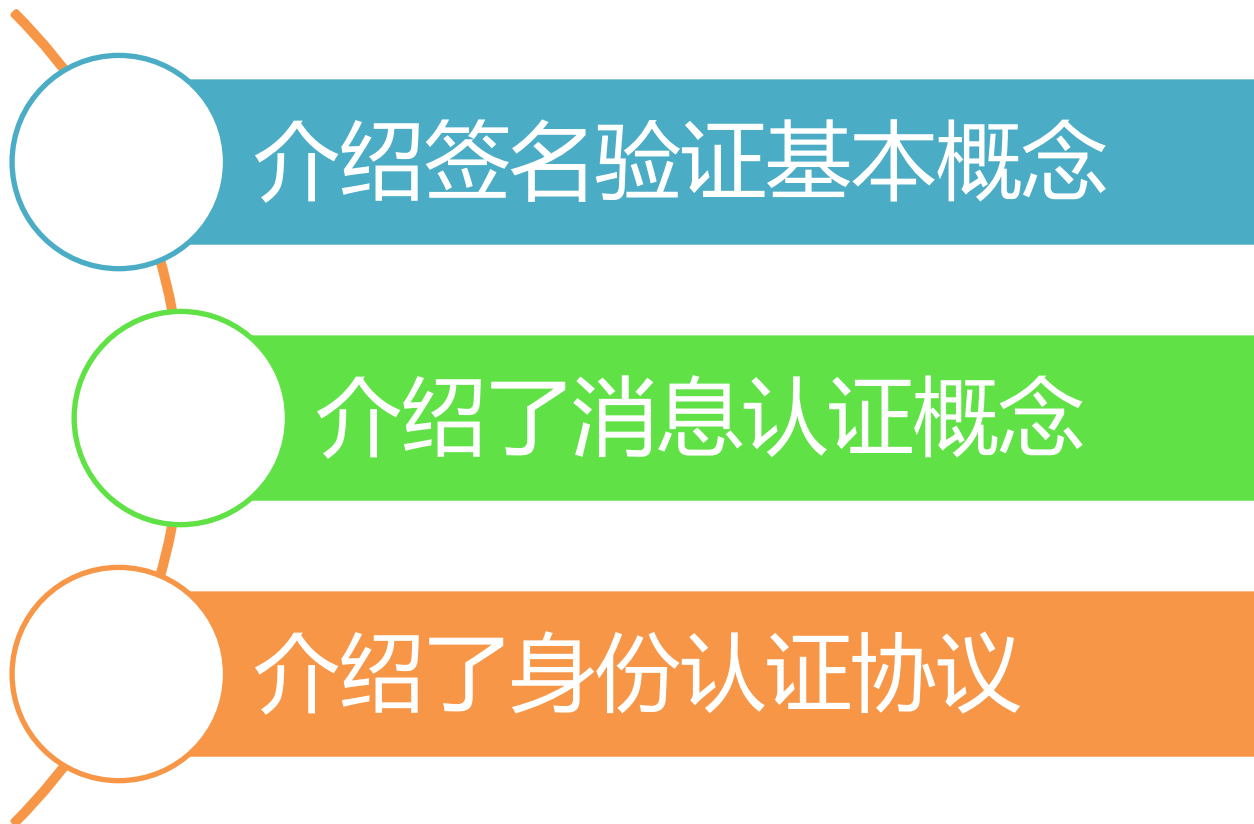
基于数字证书的身份鉴别协议

为解决非对称密钥身份鉴别技术中存在的“公开密钥真实性”的问题，可采用证书对实体的公开密钥的真实性进行保证。





第三讲 签名与认证基础知识 > 身份认证





思考题

- 1、列举3种自己使用过的身份认证方法，并比较不同方法的安全程度。
- 2、课件中基于NS的身份认证协议是存在缺陷的，假定攻击者C截取并保存 $\{A, K_A(B, K_S)\}$ ，然后监听A与B的通信报文 $K_S(M)$ ，并通过离线计算出 K_S ，此时C就获得了假冒A的能力。请简要分析原理，并给出C假冒A通过B认证的过程。
(提示：可参考阅读教材P70页的NS协议。)





本讲到此结束，谢谢聆听！



下一讲：访问控制基础知识

