

密码学

第十五讲 认证

王后珍

武汉大学国家网络安全学院

空天信息安全与可信计算教育部重点实验室





目录

- 第一讲 信息安全概论
- 第二讲 密码学的基本概念
- 第三讲 数据加密标准 (DES)
- 第四讲 高级数据加密标准 (AES)
- 第五讲 中国商用密码SM4与分组密码应用技术
- 第六讲 序列密码基础
- 第七讲 祖冲之密码
- 第八讲 中国商用密码HASH函数SM3
- 第九讲 复习





目录

第十讲 公钥密码基础

第十一讲 中国商用公钥密码SM2加密算法

第十二讲 数字签名基础

第十三讲 中国商用公钥密码SM2签名算法

第十四讲 密码协议

第十五讲 认证

第十六讲 密钥管理：对称密码密钥管理

第十七讲 密钥管理：公钥密码密钥管理

第十八讲 复习

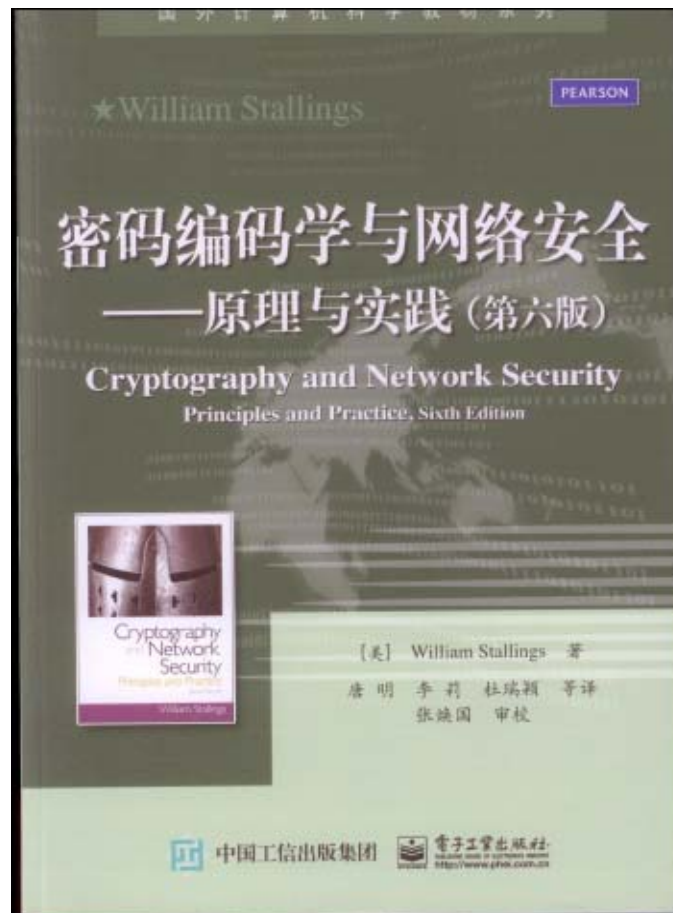


教材与主要参考书

教材



参考书



武汉大学



本讲内容

一、认证的概念

二、身份认证

三、站点认证

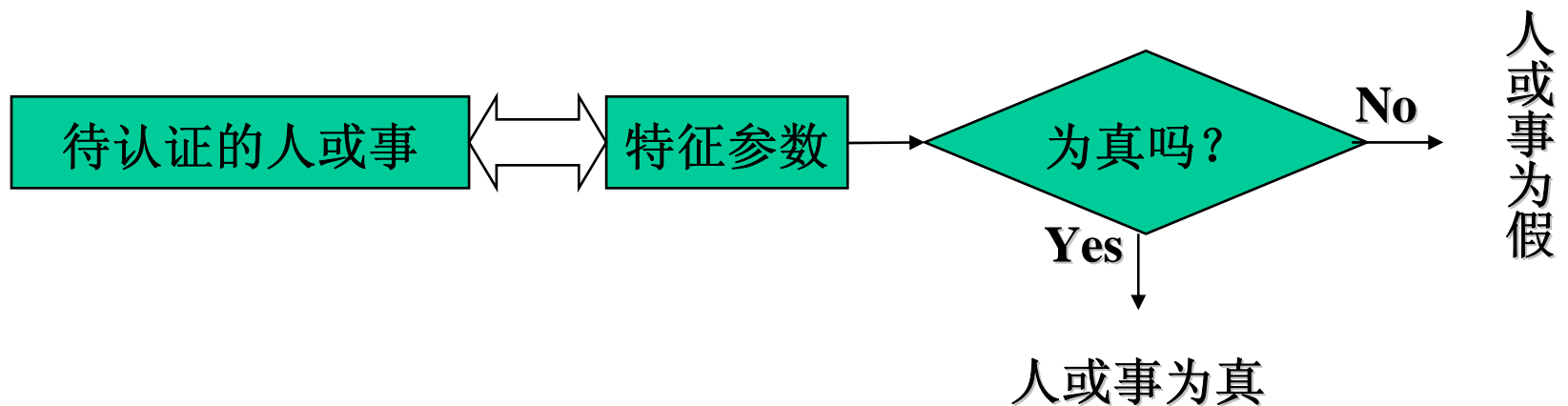
四、报文认证与消息认证码





一、认证的概念

- 认证（**Authentication**）又称鉴别，确认，它是证实某人某事是否名副其实或是否有效的一个过程。
- 认证往往是许多信息系统中安全保护的第一道设防，因而极为重要。
- 认证模型





一、认证的概念

- 常用的认证参数有口令、标识符、密钥、信物、智能卡、**USB-Key**、指纹、视网膜纹等。
- 一般说来，利用人的生理特征参数进行认证的安全性高，但技术要求也高，成本也较高。其中，指纹识别和人脸识别逐渐开始应用。
- 目前应用最广泛的还是基于密码的认证技术。
- 认证和加密的区别：
 - 加密用以确保数据的秘密性。
 - 认证用以确保当事人身份和数据的真实性。





一、认证的概念

● 认证和数字签名的区别：

- ① 认证总是基于某种收发双方共享的**保密数据**来认证对象的真实性，而数字签名中用于**验证签名的数据**是公开的。
- ② 认证允许收发双方互相验证其真实性，**不准许第三者验证**，而数字签名**允许收发双方和第三者都能验证**。
- ③ 数字签名具有发送方不能抵赖、接收方不能伪造和能够公开验证解决纠纷的能力，而认证则不一定具备。





二、身份认证

- 用户的身份认证是许多信息系统的第一道防线，其目的在于识别用户的合法性，从而阻止非法用户访问系统。
- 可见，身份认证对确保系统的信息安全是极其重要的。
- 一般，可以通过以下验证，来认证用户的身份：
 - 用户知道什么
 - 用户拥有什么
 - 用户的生理特征





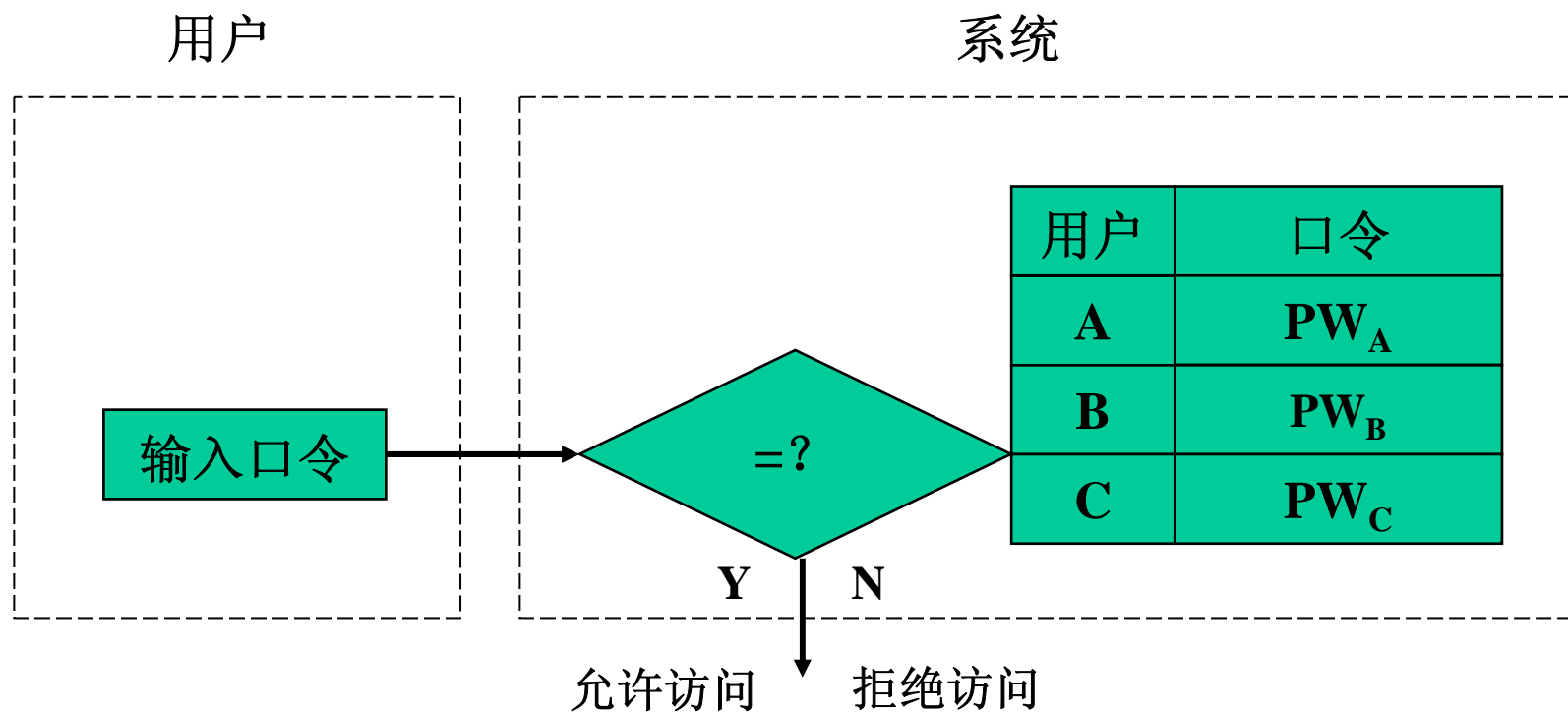
二、身份认证

1. 口令

- 口令是双方预先约定的秘密数据，口令认证属于验证用户知道什么。
- 口令验证的安全性虽然不如其他几种方法，但是口令验证简单易行，因此口令验证仍是目前应用最为广泛的身份认证方法。
- 在一些简单的系统中，用户的口令以口令表的形式存储。当用户要访问系统时，系统要求用户提供口令，系统将用户提供的口令与口令表中存储的口令进行比较，若相等则确认用户身份有效，否则确认用户身份无效，拒绝访问。



二、身份认证





二、身份认证

1. 口令

- 这样的简单口令系统存在以下问题：
 - ① 因为用户的口令以明文形式存储在系统中，系统管理员可以获得所有口令，攻击者也可利用系统的漏洞来获得他人的口令。
 - ② 因为用户的口令在用户终端到系统的线路上以明文形式传输，所以攻击者可在传输线路上截获用户口令。
 - ③ 只有系统验证用户的身份，用户不能验证系统的身份。





二、身份认证

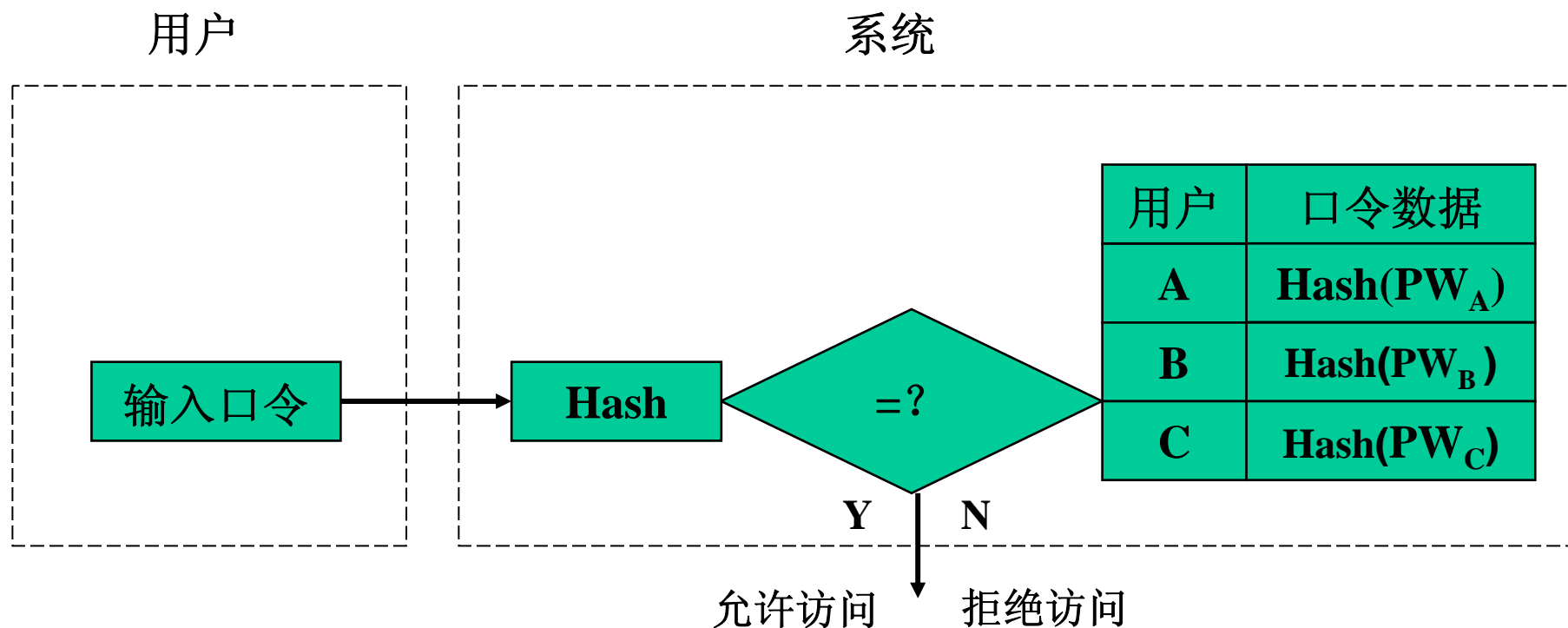
1. 口令

- 用单向函数加密口令：

- ① 用户的口令在系统中以密文的形式存储。
- ② 口令一旦加密，将永不可解密。
- ③ 用户访问系统时提供其口令，系统对该口令用单向函数加密，并与存储的密文相比较。若相等，则确认用户身份有效，否则确认用户身份无效。
- ④ 可选用强的**HASH**函数作为单向函数。



二、身份认证





二、身份认证

1. 口令

- 利用数字签名方法验证口令：

① 用户 i 将其公钥提交给系统，作为验证口令的数据，系统为每个用户建立一个已访问次数标志 T_i

② 用户访问系统时把下列签名信息提供给系统：

$$\langle ID_i \| D((ID_i, N_i), K_{di}) \rangle,$$

其中 N_i 表示本次访问是第 N_i 次访问。

③ 系统根据明文形式的标识符 ID_i 查出 K_{ei} ，并计算
 $E(D((ID_i, N_i), K_{di}), K_{ei}) = \langle ID_i^*, N_i^* \rangle$





二、身份认证

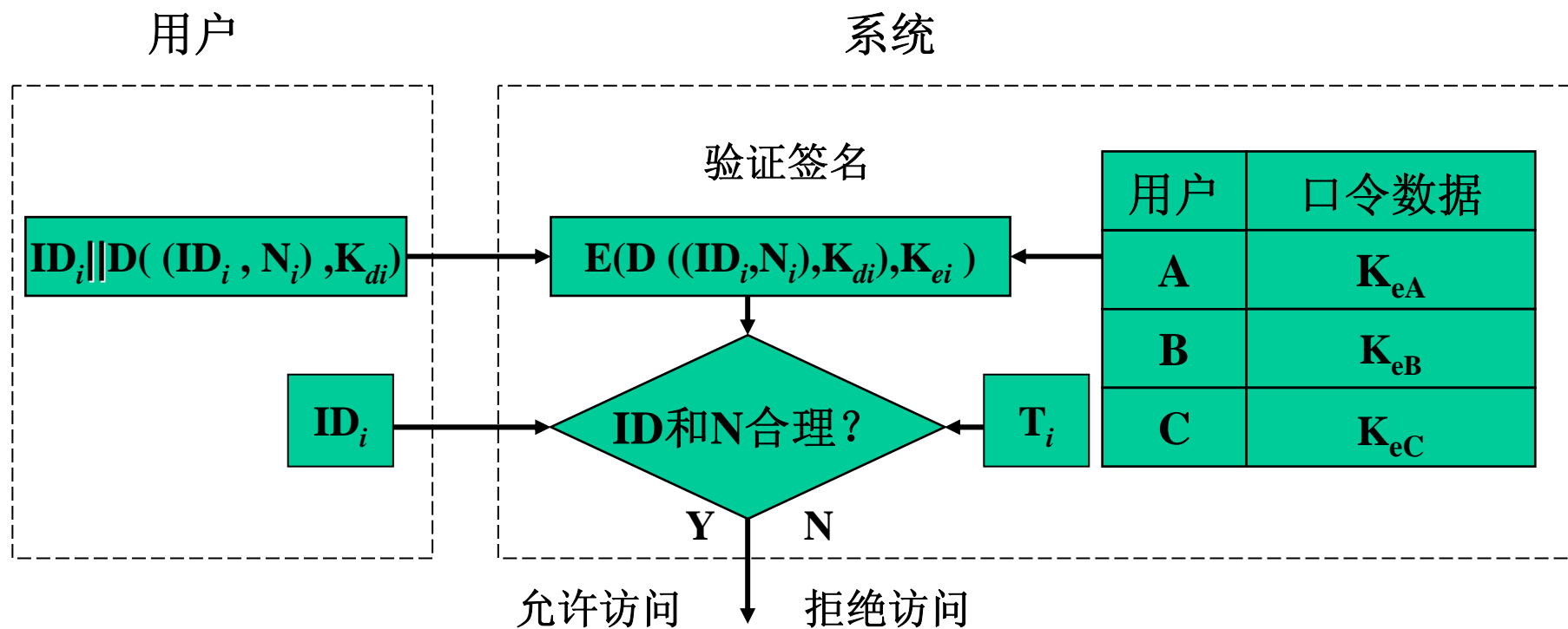
1. 口令

- 利用数字签名方法验证口令：

- ④ 当且仅当 $ID_i = ID_i^*$, $N_i^* = T_i + 1$ 时系统才确认用户身份有效。
- ⑤ 安全性分析：口令是用户的保密的解密密钥 K_{di} ，它不存储于系统中，所以其他人都不可得到；虽然 K_{ei} 存储于系统中，但是由 K_{ei} 不能推出 K_{di} ；又由于从终端到系统的通道上传输的是签名数据而不是 K_{di} 本身，所以攻击者也不能通过信道截取获得 K_{di} ；由于系统为每用户设置了已访问次数标志 T_i ，且仅当 $N_i^* = T_i + 1$ 是才接收访问，所以可以抗重播攻击。但必须对 T_i 实施保护。



二、身份认证





二、身份认证

1. 口令

- 口令的双向验证：

- 仅有系统验证用户的身份，而用户不能验证系统的身份，是不全面的，也是不平等的。
- 设A的口令为 P_A ，B的令为 P_B 。
- 当A要求与B通信时，B必须验证A的身份，因此A应当首先向B出示表示自己身份的数据。但此时A尚未对B的身份进行验证，所以A不能贸然将自己的口令发给B。
- 如果B要求与A通信也存在同样的问题。





二、身份认证

1. 口令

- 口令的双向验证：

- 设 f 是单向函数， R_A 是A的随机数， R_B 是B的随机数。
 P_A 是A的口令， P_B 是B的口令，**A和B共享口令。**

① $A \rightarrow B: R_A$

② $B \rightarrow A: f(P_B \parallel R_A) \parallel R_B$

- A利用单向函数 f 对自己的 R_A 和共享的 P_B 进行变换，得到 $f(P_B \parallel R_A)$ ，并与接收到的 $f(P_B \parallel R_A)$ 进行比较。若两者相等，则A确认B的身份为真。否则，A确认B的身份为假。





二、身份认证

1. 口令

- 口令的双向验证：

③ $A \rightarrow B: f(P_A \| R_B)$

- B利用单向函数 f 对自己的 R_B 和共享的 P_A 进行变换，得到 $f(P_A \| R_B)$ ，并与接收到的 $f(P_A \| R_B)$ 进行比较。若两者相等，则B确认A的身份为真。否则，B确认A的身份为假。

- 安全性：由于 f 是单向函数，由 $f(P_A \| R_A)$ 和 R_A 不能计算出 P_A ，由 $f(P_B \| R_B)$ 和 R_B 不能计算出 P_B ，所以在上述口令验证中，即使有一方是假冒者，由于他没有共享的密钥，故他不能骗得对方的口令。为了阻止重播攻击，可在 $f(P_B \| R_A)$ 和 $f(P_A \| R_B)$ 中加入时间参量。





二、身份认证

1. 口令

● 一次性口令：

- 为了安全，口令应当经常更换，最好是一个口令只使用一次。利用单向函数可实现一次性口令。
- 设A和B要进行通信，A选择随机数 x ，并计算 $y_0=f^n(x)$
- A将 y_0 发送给B作为验证口令的数据。因为 f 是单向函数，所以对 y_0 不需保密。
- A以

$$y_i=f^{n-i}(x) \quad (1 \leq i \leq n-1)$$

作为其第 i 次通信的口令发送给B。

- B计算并验证： $f(y_i)=y_{i-1}$ 吗？若相等，则确认A的身份是真实的，否则可知A的身份是不真实的，





二、身份认证

2. 磁卡、智能卡和USB-Key

这类认证是验证用户拥有什么。

- 磁卡：

- 磁卡是目前已广泛应用的一种个人身份持证物，在银行界得到广泛地应用。磁卡使用方便、成本低。但磁卡仅有有限的数据存储能力，无数据处理能力，安全性低。





二、身份认证

2. 磁卡、智能卡和USB-Key

- 智能卡：

- 智能卡是一种镶嵌有单片机芯片的集成电路卡。卡上有CPU、RAM、EEPROM或FLASH、ROM和I/O接口。因此智能卡被誉为最小的个人计算机。芯片操作系统COS（Chip Operating System）管理资源。安全性高。





二、身份认证

2. 磁卡、智能卡和USB-Key

- **USB-Key :**

- **USB-Key**是一种具有**USB** 接口，具有加解密、数字签名等多种安全保密功能的便携式安全设备。从技术上看，**USB-Key**就是一个具有**USB**接口智能卡。





二、身份认证

2. 磁卡、智能卡和USB-Key

- 如果仅仅只靠磁卡、智能卡和USB-key这种物理持物来作为用户的身份凭证进行身份认证，尚有不足。因为它们会丢失，则捡到的人就可假冒真正的用户。
- 因此，还需要一种磁卡、智能卡和USB-key上不具有的身份信息。这种身份信息通常采用个人识别号PIN(Personal Identification Number)。





二、身份认证

3. 生理特征识别

- 人的指纹、掌纹、面孔、发音、视网膜、**DNA**等都具有唯一性和稳定性的特征，即每个人的这些特征都与别人不同且终生不变，因此可以据此进行身份识别。
- 基于这些生理特征，人们发展了指纹识别、视网膜识别、语音识别、人脸识别等多种生物识别技术，其中指纹识别和人脸识别技术比较成熟，开始得到应用。





零知识证明

- “零知识证明”—zero-knowledge proof
- 零知识证明由Goldwasser等人在20世纪80年代初提出的。
- 它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。





零知识证明

- 零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。
- 证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。
- 大量事实证明，零知识证明在密码学中非常有用。如果能够将零知识证明用于验证，将可以有效解决许多问题。





零知识证明

- 设 P 是示证者， V 是验证者， P 可通过两种方法向 V 证明他知道某种秘密信息。
- 一种方法是 P 向 V 说出该信息，但这样 V 也就知道了该秘密。
- 另一种方法是采用交互证明方法，它以某种有效的数学方法，使 V 确信 P 知道该秘密，而 P 又不泄露其秘密，这即是所谓的零知识证明。





零知识证明

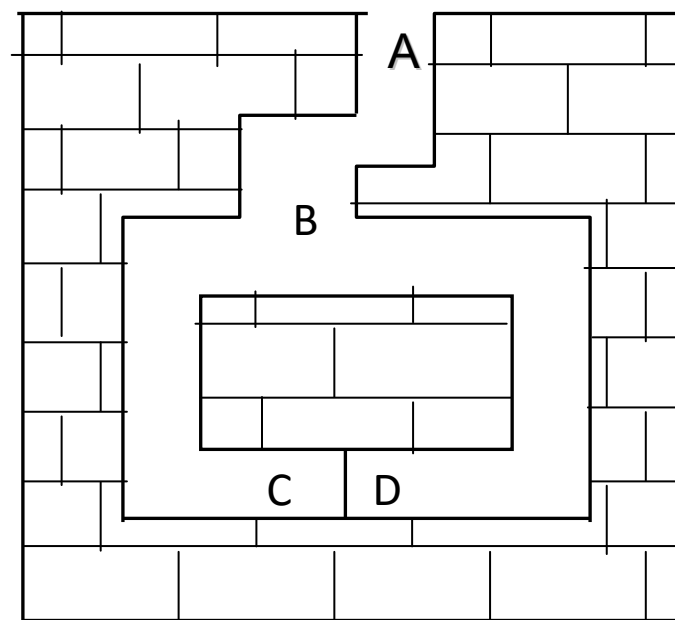


图8—4 零知识洞穴





零知识证明的概念

设 P 表示掌握某些信息，并希望证实这一事实的实体，设 V 是证明这一事实的实体。

- 某个协议向 V 证明 P 的确掌握某些信息，但 V 无法推断出这些信息是什么，我们称 P 实现了**最小泄露证明**。
- 如果 V 除了知道 P 能够证明某一事实外，不能够得到其他任何知识，我们称 P 实现了**零知识证明**，相应的协议称作**零知识协议**。



武汉大学



零知识证明的概念

- 在最小泄露协议中满足下述两个性质：
 - (1) **P无法欺骗V**。换言之，若P不知道一个定理的证明方法，则P使V相信他会证明定理的概率很低。
(正确性)
 - (2) **V无法欺骗P**。换言之，若P知道一个定理的证明方法，则P使V以绝对优势的的概率相信他能证明。
(完备性)
- 在零知识协议中，除满足上述两个条件以外，还满足下述性质：
 - (3) V无法获取任何额外的知识。 (**零知识性**)



武汉大学



零知识洞穴

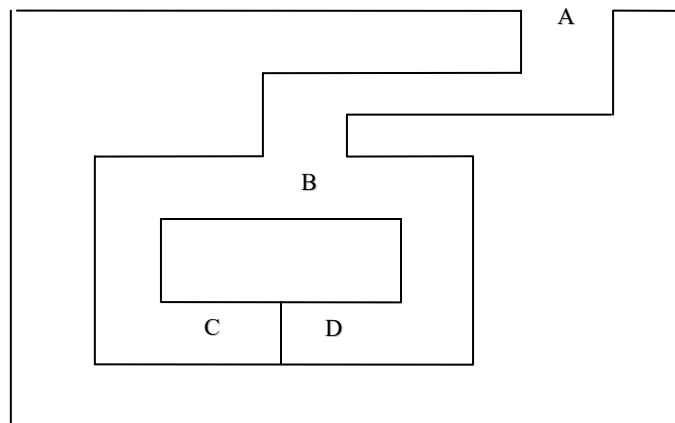
- 设P知道咒语，可打开C和D之间的秘密门，不知道者则走向死胡同。现在来看P如何向V出示证明使其相信他知道这个秘密，但又不告诉V有关咒语。
- 协议1：洞穴协议
 - V站在A点；
 - P进入任一点C或D；
 - 当P进洞之后，V走向B点；
 - V叫P：(a)从左边出来，或(b)从右边出来
 - P按照要求实现（有咒语）；
 - P和V重复执行(1)~(5)共 n 次。



武汉大学



零知识洞穴



- 若P不知道咒语，则在B点，只有50%的机会猜中V的要求，协议执行 n 次，则只有 2^{-n} 次机会完全猜中。此洞穴问题可以转化为数学问题，P知道解决某个难题的秘密信息，而V通过与P交互作用验证其真伪。



武汉大学



交互式零知识证明



- 证明者和验证者共享输入 (函数或者是值)
- 如果验证者检查, 对于每一个挑战的响应都是正确的, 这个协议才输出Accept, 否则, 输出 Reject



武汉大学



平方根问题的零知识

- 令 $N = P Q$, P 、 Q 为两个大素数, Y 是 $\text{mod } N$ 的一个平方, 且 $\text{gcd}(Y, N) = 1$, **注意找到 $\text{mod } N$ 的平方根与分解 N 等价**。
- Peggy声称他知道 Y 的一个平方根 S , 但他不愿意泄露 S , Vector想证明Peggy是否真的知道。下面给出了这个问题的一个解决方案。
 - Peggy选择两个随机数 R_1 和 R_2 , 满足 $\text{gcd}(R_1, N) = 1$, $R_2 = S R_1^{-1}$, $R_1 R_2 = S \pmod{N}$ 。Peggy计算 $X_1 = R_1^2 \pmod{N}$, $X_2 = R_2^2 \pmod{N}$, 并将 X_1 、 X_2 发送给Vector。
 - Vector检验 $X_1 X_2 = Y \pmod{N}$, 然后Vector随机选择 X_1 (或 X_2) 让Peggy提供它的一个平方根, 并检验Peggy是否提供的是真的平方根。
 - 重复上面的过程直至Vector相信。
- 如果, Peggy不知道 Y 的平方根, 虽然他可能知道 X_1 、 X_2 的一个平方根, 但不是全部。



武汉大学

离散对数问题的零知识证明

Peggy试图向Vector证明他知道离散对数 x , $x = \log_g Y \bmod p$, $Y = g^x \bmod p$

$$x = \log_g Y \bmod p, \quad (Y = g^x \bmod p)$$

Prover

Verifier

$$t \in_R Z_q^*$$

$$R = g^t \bmod p$$

$$w = t - ux \bmod q$$

R **Commitment**

u **Challenge**

w **Response**

$$u \in_R Z_q^*$$

$$R \stackrel{?}{=} g^w Y^u \bmod p$$



离散对数问题的零知识证明

Peggy试图向Vector证明两个离散对数相等而不泄露 x ,

$$Y = g^x, Z = c^x, \log_g Y = \log_c Z$$

Prover

$$\begin{array}{l} Y = g^x, Z = c^x \\ \log_g Y = \log_c Z \end{array}$$

Verifier

$$t \in_R Z_q^*$$

$$R_1 = g^t \bmod p$$

$$R_2 = c^t \bmod p$$

$$w = t - ux \bmod q$$

R_1, R_2 **Commitment**

u **Challenge**

W **Response**

$$u \in_R Z_q^*$$

$$R_1 = g^w Y^u \bmod p$$

$$R_2 = c^w Z^u \bmod p$$



武汉大学



证明ElGamal解密的正确性

比如，Peggy试图证明他的ElGamal解密是正确的。

- 明文是 m 而不泄露他的私钥 x 。

Peggy的公钥为 $Y = g^x \bmod p$;

- ElGamal加密为 $m \rightarrow (U, V)$, $U = g^r \bmod p$

$$V = mY^r \bmod p$$

- ElGamal解密为 $V / U^x \rightarrow m$

- Peggy只需证明下面的两个离散对数相等即可： $Y = g^x$, $V / m = U^x$, $\log_g Y = \log_g U (V / m)$ 。



非交互零知识证明

- 使用 Fiat-Shamir Heuristic的非交互零知识证明 (NIZK)

$$x = \log_g Y \bmod p, \quad (Y = g^x \bmod p)$$

Prover

$$t \in_R Z_q^*$$

$$R = g^t \bmod p$$

$$u = H(Y, R)$$

$$w = t - ux \bmod q$$

Verifier

$$u = H(Y, R)$$

$$R \stackrel{?}{=} g^w Y^u \bmod p$$



武汉大学



身份鉴别方案

- 在一个安全的身份认证协议中，我们希望被认证者 P 能向验证者 V 电子地证明他的身份，而又不向 P 泄露他的认证信息
- Feige-Fiat-Shamir身份鉴别方案
- Guillou-Quisquater身份鉴别方案
- Schnorr身份鉴别方案



武汉大学



简化的Feige-Fiat-Shamir身份鉴别方案

- 可信赖仲裁方选定一个随机模数 $n = p_1 \times p_2$, p_1 、 p_2 为两个大素数。实际中 n 至少为512比特, 尽量长达1024比特。仲裁方可实施公钥和私钥的分配。他产生随机数 v (v 为对模 n 的二次剩余)。
- 换言之, 选择 v 使得 $x^2 = v \pmod n$ 有一个解并且 $v^{-1} \pmod n$ 存在。以 v 作为被验证方的公钥, 而后计算最小的整数 s : $s \equiv \text{sqrt}(v^{-1}) \pmod n$, 将它作为被验方P的私人密钥而分发给他。



武汉大学



简化的Feige-Fiat-Shamir身份鉴别方案

- 实施身份证明的协议如下：
 - (1) 用户P取随机数 r ($r < n$)，计算 $a = (r^2) \bmod n$ ，送给验证方V；
 - (2) V将随机比特 b 送给P；
 - (3) 若 $b = 0$ ，则P将 r 送给V；若 $b = 1$ ，则将 $y = r s \bmod n$ 送给V；
 - (4) 若 $b = 0$ ，则V验证 $a = r^2 \bmod n$ ，从而证明P知道 $\text{sqrt}(a)$ ；若 $b = 1$ ，则V验证 $a = y^2 \bmod n$ ，从而**证明P知道 s** 。
- 这是一轮认证，P和V可将此协议重复 t 次，直到V确信P知道 s 为止。



武汉大学



简化的Feige-Fiat-Shamir身份鉴别方案

A

B

$$\xrightarrow{x \equiv r^2 \pmod{n}}$$

$$\xleftarrow{e \in \{0, 1\}}$$

$$\xrightarrow{y \equiv r \cdot s^e \pmod{n}}$$

If $y \neq 0$ and $y^2 \equiv x \cdot v^{-e} \pmod{n}$,
then B accepts the proof;
otherwise, B rejects the proof.



武汉大学



简化的Feige-Fiat-Shamir身份鉴别方案

- 安全性讨论如下：
 - P欺骗V的可能性。P不知道 s ，他也可选取随机数 r ，将 $x = r^2 \bmod n$ 发给V，V发送随机比特 b 给P，P可将 r 送出。当 $b = 0$ 时，则V让P通过检验而受骗；当 $b = 1$ 时，则V可发现P不知道 s 。V受骗的概率为 $1/2$ ，但连续 t 次受骗的概率将仅为 2^{-t} 。
 - V伪装P的可能性。V和其他验证者W开始一个协议。第一步他可用P用过的随机数 r ，若W所选的 b 值恰与以前发给P的一样，则V可将在第(3)步所发的 r 或 y 重发给W，从而可成功的伪装P。但W可能随机地选 b 为0或1，故这种工具成功的概率为 $1/2$ ，执行 t 次，则可使其降为 2^{-t} 。



武汉大学



Feige-Fiat-Shamir身份鉴别方案

- 可信赖仲裁方选 $n = p_1 \times p_2$, p_1 、 p_2 为两个大素数, 并选 k 个不同的随机数 v_1, v_2, \dots, v_k , 各 v_i 是 $\text{mod } n$ 的平方剩余, 且有逆。以 v_1, v_2, \dots, v_k 为被验证方P的公钥, 计算最小正整数 s_i , 使 $s_i = \sqrt{1/v_i} \text{ mod } n$, 将 s_1, s_2, \dots, s_k 作为P的私钥。



武汉大学



Feige-Fiat-Shamir身份鉴别方案

- 协议如下：
 - (1) P选随机数 r ($r < m$)，计算 $x = r^2 \bmod n$ 并发送给验证方V；
 - (2) V选 k 比特随机二进制串 b_1, b_2, \dots, b_k 传送给P；
 - (3) P计算 $y = r \times (s_1^{b_1} \times s_2^{b_2} \times \dots \times s_k^{b_k}) \bmod n$ ，并送给V；
 - (4) V验证 $x = y^2 \times (v_1^{b_1} \times v_2^{b_2} \times \dots \times v_k^{b_k}) \bmod n$ 。
- 此协议可执行 t 次，直到V相信P知道 s_1, s_2, \dots, s_k ，P欺骗V的机会为 2^{-kt} 。



武汉大学



Feige-Fiat-Shamir身份鉴别方案

A

B

$$x \equiv r^2 \pmod{n}$$

$$(e_1, \dots, e_k), e_i \in \{0, 1\}$$

$$y \equiv r \cdot \prod_{e_j=1} s_j \pmod{n}$$

If $z \equiv y^2 \cdot \prod_{e_j=1} v_j^{e_j} \not\equiv 0 \pmod{n}$ and $z = x$,
then *B* accepts the proof;
otherwise, *B* rejects the proof.



武汉大学



Guillo-Quisquater身份鉴别方案

- Guillo和Quisquater给出一种身份认证方案，这个协议需要三方参与、三次传送，利用公钥体制实现。
- 可信赖仲裁方T先选定RSA的秘密参数 p 和 q ，生成大整数模 $n = p q$ 。公钥指数有 $e \geq 3$ ，其中 $\gcd(\phi, e) = 1$ ， $\phi = (p - 1)(q - 1)$ 。计算出秘密指数 $d = e^{-1} \bmod \phi$ ，公开 (e, n) ，各用户选定自己的参数。
- 用户A的唯一性身份 I_A ，通过散列函数 H 变换得出相应散列值 $J_A = H(I_A)$ ， $I < J_A < n$ ， $\gcd(J_A, \phi) = 1$ ，T向A分配密钥函数 $S_A = (J_A)^d \bmod n$ 。



武汉大学



Guillo-Quisquater身份鉴别方案

- 单轮 ($t = 1$) GQ协议三次传输的消息为:
 - (1) $A \rightarrow B$: I_A , $x = r^e \bmod n$, 其中 r 是A选择的秘密随机数;
 - (2) $B \rightarrow A$: B选随机数 u , $u \geq 1$;
 - (3) $A \rightarrow B$: $y = r \cdot S_A^u \bmod n$ 。
- 具体协议描述如下:
 - (1) A选择随机数 r , $1 \leq r \leq n-1$, 计算 $x = r^e \bmod n$, A将 (I_A, x) 送给B;
 - (2) B选择随机数 u , $1 \leq u \leq e$, 将 u 送给A;
 - (3) A计算 $y = r \cdot S_A^u \bmod n$, 送给B;
 - (4) B收到 y 后, 从 I_A 计算 $J_A = H(I_A)$, 并计算 $J_A^u \cdot y^e \bmod n$ 。
- 若结果不为0且等于 x , 则可确认A的身份; 否则拒绝A。



武汉大学



Guillo-Quisquater身份鉴别方案

A

$$\underline{I_A, x \equiv r^e \pmod{n}}$$

u , where $1 \leq u \leq v$



$$\underline{y \equiv r \cdot s_A^u \pmod{n}}$$

B

If $z \equiv J_A^u \cdot y^e \not\equiv 0 \pmod{n}$ and $z \equiv x$,
then *B* accepts the proof;
otherwise, *B* rejects the proof.



武汉大学



Schnorr身份鉴别方案

- 以上方案有一定的缺陷：实时计算量、消息交换量和所需存储量较大，Schnorr提出的一种安全性基于计算离散对数的困难性的鉴别方案，可以做预计算来降低实时计算量，所需传送的数据量亦减少许多，特别适用于计算能力有限的情况。
- Claus Schnorr的认证方案的安全性建立在计算离散对数的难度上。
- 为了产生密钥对，首先选定系统的参数：素数 p 及素数 q ， q 是 $p-1$ 的素数因子。 $p = 2^{1024}$ ， $q > 2^{160}$ ，元素 g 为 q 阶元素， $1 \leq g \leq p-1$ 。令 a 为 $GF(p)$ 的生成元，则得到 $g = a^{(p-1)/q} \bmod p$ 。由可信赖的第三方 T 向各用户分发系统参数 (p, q, g) 和验证函数（即 T 的公钥），用此验证 T 对消息的签字。



武汉大学



Schnorr身份鉴别方案

- 对每个用户给定惟一身份 I ，用户A选定秘密密钥 s ， $0 \leq s \leq q-1$ ，并计算 $v = g^{-s} \bmod p$ ；A将 I_A 和 v 可靠地送给T，并从T获得证书， $C_A = (I_A, v, S_T(I_A, v))$ 。
- 协议如下：
 - (1) 选定随机数 r ， $1 \leq r \leq q-1$ ，计算 $x = g^r \bmod p$ ，这是预处理步骤，可在B出现之前完成；
 - (2) A将 (C_A, x) 送给B；
 - (3) B以T的公钥解 $S_T(I_A, v)$ ，实现对A的身份 I_A 和公钥 v 认证，并传送一个介于0到 2^t-1 之间的随机数 e 给A；
 - (4) A验证 $1 \leq e \leq 2^t$ ，计算 $y = (s e + r) \bmod q$ ，并将 y 送给B；
 - (5) B验证 $x = g^y v^e \bmod p$ ，若该等式成立，则认可A的身份合法。
- 安全性基于参数 t ， t 要选得足够大以使正确猜对 e 的概率 2^{-t} 足够小。Schnorr建议 t 为72位， p 大约为512位， q 为140位。
- 此协议是一种对 s 的零知识证明，在认证过程中没有暴露有关 s 的任何有用信息。



武汉大学



Schnorr身份鉴别方案

A

$$C_A, x \equiv y^r \pmod{p}$$



$$e, \text{ where } 1 \leq e \leq 2^t < q$$



$$y \equiv s \cdot e + r \pmod{q}$$



B

If $x \equiv g^y \cdot v^e \equiv x \pmod{p}$,
then B accepts the proof;
otherwise, B rejects the proof.



武汉大学



复杂性理论

- 在计算机学科中，存在多项式时间的算法的一类问题，称之为P类问题；而向旅行商问题、命题表达式可满足问题这类，至今没有找到多项式时间算法解的一类问题，称之为NP类问题。
- NP问题中最难的称之为NP完全问题
 - (1) 旅行商问题
 - (2) 三方匹配问题
 - (3) 三方满足问题



武汉大学



NP与零知识证明

- 每一个NP问题都存在一个零知识证明
- GMR(Goldwasser, Micali, Rackoff)
 - “The knowledge complexity of interactive-proof systems”, Proc. of 17th ACM Sym. on Theory of Computation, pp.291-304, 1985
 - “The knowledge complexity of interactive-proof systems”, Siam J. on Computation, Vol. 18, pp.186-208, 1989 (revised version)

•



武汉大学



三、站点认证

- 为了确保通信安全，在正式传送报文之前，应首先认证通信是否在意定的站点之间进行，这一过程称为**站点认证**。
- 站点认证是通过验证加密的数据能否正确地在两个站点间进行传送来实现的。



三、站点认证

- 设A、B是意定的两个站点，A是发送方，B是接收方。利用传统密码体制，则A和B相互认证的过程如下：

- 假定A、B共享保密的会话密钥 K_S

A方：

B方：

- | | |
|-----------------------------|----------------------------------|
| 1. A产生随机数 R_A | 1. B产生随机数 R_B |
| 2. A → B: $E(R_A, K_S)$ | 2. B接收 $E(R_A, K_S)$ ，并解密出 R_A |
| 3. A接收 $E(R_A R_B, K_S)$ | 3. B → A: $E(R_A R_B, K_S)$ |
| 并解密判断 $R_A = R_A$? | 4. B接收 $E(R_B, K_S)$ ，并解密出 R_B |
| 若相等则A认为B是合法站点。 | 5. B判断 $R_B = R_B$? |
| 4. A → B: $E(R_B, K_S)$ | |

若相等则B认为A是合法站点。

- 安全性：上述协议成功执行，则表明A拥有 K_S 且B也拥有 K_S ， K_S 是保密的，因此A、B是合法的。任何其他人却没有共享的会话密钥 K_S ，所以不能冒充A和B正确执行上述协议。





三、站点认证

● 利用公钥密码，则A和B相互认证的过程如下：

- | | |
|--|---|
| 1. A产生随机数 R_A | 1. B产生随机数 R_B |
| 2. A → B: R_A | 2. B接收 R_A |
| 3. A接收 $D(R_A R_B, K_{dB})$
并验证B的签名，
如正确则A认为B是合法站点。 | 3. B → A: $D(R_A R_B, K_{dB})$ |
| 4. A → B: $D(R_B, K_{dA})$ | 4. B接收 $D(R_B, K_{dA})$
并验证A的签名，如正确则B认为A是合法站点。 |

● 安全性：上述认证本质上是验证数字签名，数字签名具有确保真实性的能力。





四、报文认证

- 报文认证必须使通信方能够验证每份报文的发送方、接收方、内容和时间性的真实性和完整性。使之能够确定：
 - (1) 报文是由意定的发送方发出的；
 - (2) 报文传送给意定的接收方；
 - (3) 报文内容有无篡改或发生错误；
 - (4) 报文按确定的次序接收。





四、报文认证

1、报文源的认证

① 采用传统密码

- 设A为发送方，B为接收方。**A和B共享保密的密钥 K_S** 。
- 设A的标识为 ID_A ，报文为 M ，在报文中增加标识 ID_A ，那么B认证A的过程如下：
$$A \rightarrow B: \langle ID_A, E(ID_A \| M, K_S) \rangle$$
- B收到报文后用 K_S 解密，**若解密所得的发送方标识与明文的 ID_A 相等，则B认为报文是A发来的。**





四、报文认证

1、报文源的认证

② 采用公开密钥密码

- 报文源的认证十分简单。只要发送方对每一报文进行数字签名，接收方验证签名即可：
 - $A \rightarrow B: \langle ID_A, D(ID_A \| M, K_{dA}) \rangle$
 - B: 验证签名, $E(D(ID_A \| M, K_{dA}), K_{eA})$, 并检验所得 ID_A 是否等于明文 ID_A ? 若验证签名正确, 则认为发方A为真。
 - 注意: 此方案不能保密, 因为 K_{eA} 是公开的, 任何人都可以得到, 并加密得到 M 。





四、报文认证

2、报文宿的认证

- 只要将报文源的认证方法稍加修改便可实现报文宿的认证。

① 采用传统密码

- 在每份报文中加入接收方标识符 ID_B ，并加密：

$$A \rightarrow B: \langle ID_B, E(ID_B \| M, K_S) \rangle$$


② 若采用公开密钥密码

- 对每份报文加入接收方标识符 ID_B ，并用B的公开加密钥进行加密：

$$A \rightarrow B: E(ID_B \| M, K_{eB})$$

- **注意：**此方案不能保真，因为 K_{eB} 是公开的，任何人都可以冒充A，发送 $E(ID_B \| M, K_{eB})$ 。






四、报文认证与消息认证码

3、报文内容的认证

- 报文内容认证使接收方能够确认报文内容的真实性和完整性，这可以通过验证消息认证码 的正确性来实现。
- **消息认证码MAC** (Message Authentication Code) 是消息内容和密钥的公开函数，其输出是固定长度的短数据块：

$$MAC = C(M, K)$$





四、报文认证与消息认证码

3、报文内容的认证

- 通信双方共享秘密钥 K ，A计算 MAC 并将报文 M 和 MAC 发送给接收方：

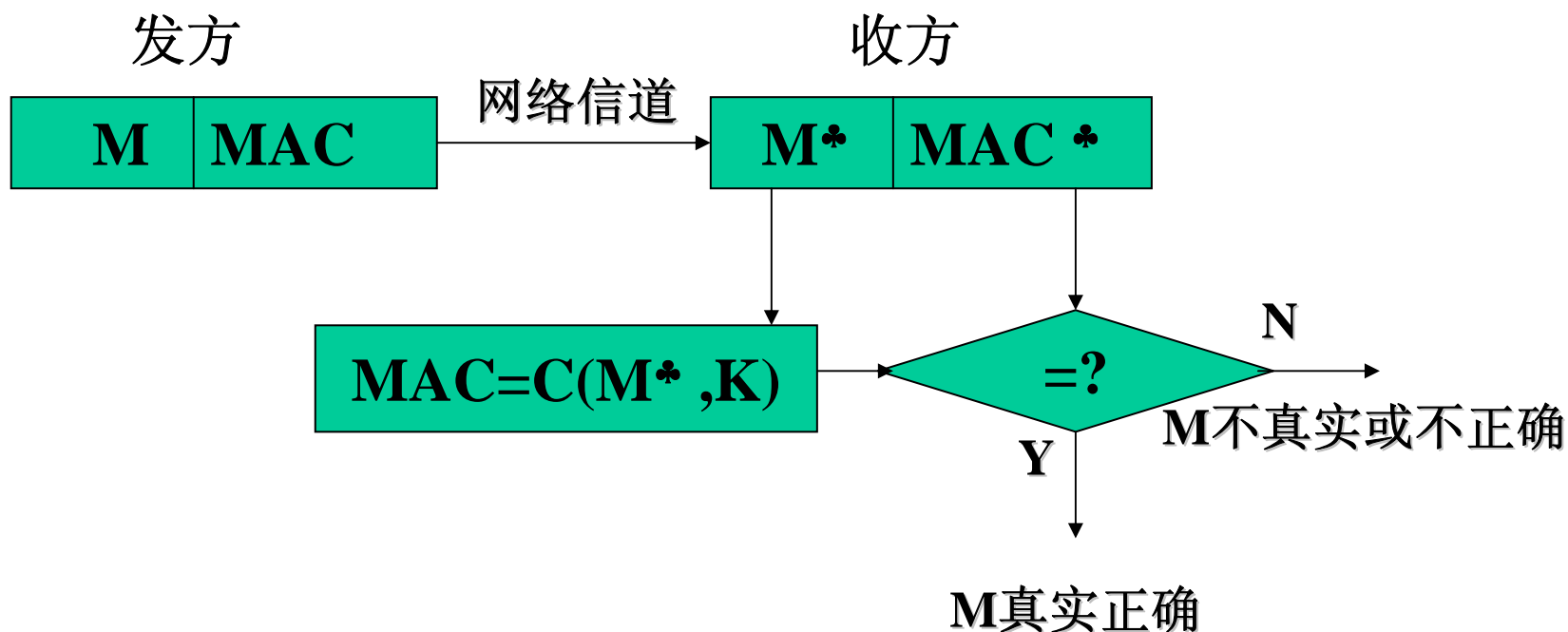
A→B: $\langle M \parallel MAC \rangle$


- 接收方收到报文 M 后用相同的秘密钥 K 重新计算得出新的 MAC ，并将其与接收到的 MAC 进行比较，若二者相等，则认为报文是真实的完整的。
- **安全性：**由于计算 MAC 需要密钥，攻击者可以篡改报文 M ，但无法计算其 MAC 。为了组织重放攻击，需要在 MAC 中加入时间参数。



四、报文认证与消息认证码

3、报文内容的认证





四、报文认证与消息认证码

3、报文内容的认证

- 在上述方法中，报文是以明文形式传送的，所以该方法可以提供认证，但不能提供保密性。
- 若要获得保密可在MAC算法之后对报文加密：


$$A \rightarrow B: E(M \parallel MAC, K_2)$$

$$\text{其中 } MAC = C(M, K_1)$$

- 安全性分析

- 因为只有A和B共享 K_1 ，所以可提供认证；
- 因为只有A和B共享 K_2 ，所以可提供保密。






四、报文认证与消息认证码

3、报文内容的认证

●注意：

- MAC 算法不要求可逆，而加密算法必须可逆；
- 由于采用传统密码，收发双方共享密钥，因此 MAC 算法不能提供数字签名功能。
- 理论上，对不同的 M ，应产生不同的 MAC 。否则，若 $M_1 \neq M_2$ ，而 $MAC_1 = MAC_2$ ，则攻击者可将 M_1 篡改为 M_2 ，而接收方不能发现。
- 但是要使函数 C 具备上述性质，将要求报文认证码 MAC 至少和报文 M 一样长，这是不方便的。





四、报文认证与消息认证码

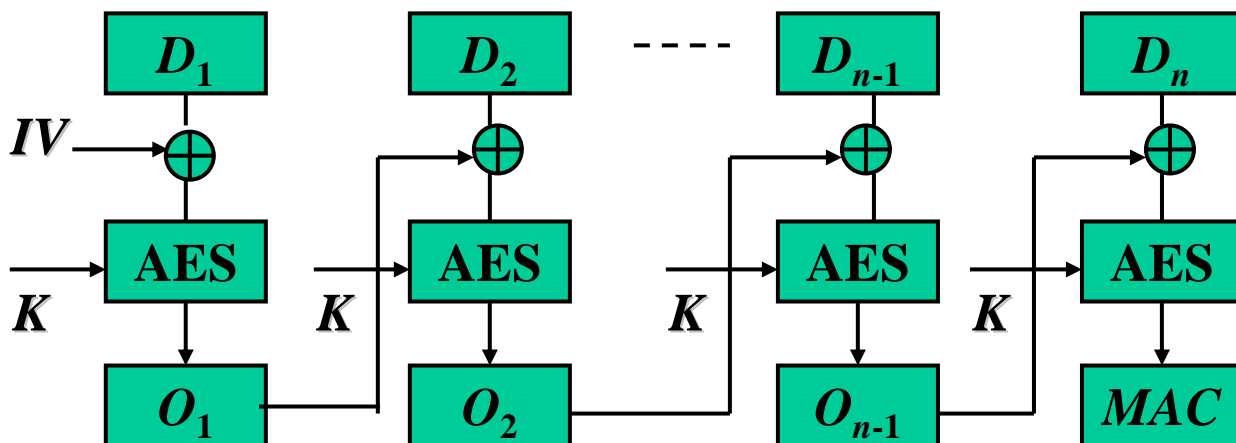
- 实际应用时要求函数 C 具有以下性质：
 - 对已知 M_1 和 MAC_1 构造满足 $MAC_2=MAC_1$ 的 M_2 在计算上是不可行的；
 - MAC 函数应是均匀分布的，即对任何随机的报文 M_1 和 M_2 ， $MAC_1=MAC_2$ 的概率是 2^{-n} ，其中 n 是 MAC 的位数；
 - 设 M_2 是 M_1 的某个已知的变换，即 $M_2=f(M_1)$ ，如 f 改变 M_1 的一位或多位，那么 $MAC_1=MAC_2$ 的概率 2^{-n} 。




四、报文认证与消息认证码

4. 利用强的分组密码产生MAC

- 用AES等强分组密码按CBC加密，产生MAC。
- 需认证的数据被分成128位的分组 $D_1\|D_2\|\dots\|D_N$ ，若最后分组不足128位，则在其后填0直至成为128位的分组。





四、报文认证与消息认证码

■ 其中, $O_1 = \text{AES}(D_1 \oplus IV, K)$


$$O_i = \text{AES}(D_i \oplus O_{i-1}, K) \quad (2 \leq i \leq N)$$

$$MAC = O_n$$

IV为初始向量, 可以取为0; K 为密钥。

- 很容易用其它强的分组密码 (如SM4) 来计算产生 MAC 。





四、报文认证与消息认证码

5. 用HASH函数产生MAC


- 简单Hash MAC
- 带密钥的HMAC

① 基于简单Hash MAC的报文认证

设A, B共享密钥 K :

$$A \rightarrow B: \langle M \parallel E(\text{Hash}(M), K) \rangle$$

- 发方计算报文 M 的 $\text{Hash}(M)$ 并使用传统密码对其加密, 将加密后的结果附于消 M 之后发送给接收方。
- B由收到的 M 重新计算 $\text{Hash}(M)$, 再加密, 并与接受到的 $E(\text{Hash}(M), K)$ 比较, 若相同则认为报文是真的。
- $\text{Hash}(M)$ 受密码保护, 没有密钥的人篡改 M 将被发现。
- 注意: 此方案没有保密功能, 因为 M 是明文。



四、报文认证与消息认证码


- 保密认证

设A，B共享密钥 K ：

$A \rightarrow B: \langle ID_A, E(ID_A \parallel M \parallel \text{Hash}(M), K) \rangle$

- 由于只有A和B共享秘密钥，所以B可以解密，如果B验证 ID_A 正确，便认证了报文源。
- B根据 M 计算新的 $\text{Hash}(M)$ ，并与接收到的 $\text{Hash}(M)$ 比较，如果相等，则可认证报文 M 的真实性和完整性。
- 由于该方法是对整个报文 M 和 $\text{Hash}(M)$ 加密，所以也提供了保密性。





四、报文认证与消息认证码


● 数字签名与认证

A→B: $\langle ID_A \parallel M \parallel D(\text{Hash}(M), K_{dA}) \rangle$

- B 根据 ID_A 用 A 的公钥 K_{eA} 验证签名，得到 $\text{Hash}(M)$ 。对收到的 M 重新计算 $\text{HASH}(M)$ 码，并与接收到的比较。如果两者相等，则可断定 M 是真实的完整的。

- 由于发方 A 进行了签名，所以该方法也提供了数字签名。A 不能抵赖，其他人不能伪造，还可以解决纠纷。

- 注意：此方案没有保密功能，因为 M 没有加密。



四、报文认证与消息认证码


- 数字签名与认证

- 改进方案

$A \rightarrow B: \langle E(ID_A \| M \| D(\text{Hash}(M), K_{dA}), K_{eB}) \rangle$

- 由于有A的签名，所以可以确保M的**真实性和完整性**。
- 由于采用了加密，所以**确保了M的秘密性**。





四、报文认证与消息认证码

② HMAC

- 带密钥的Hash函数消息认证码HMAC定义为:

$$HMAC = H[(K^+ \oplus opad) \parallel H[(K^+ \oplus ipad) \parallel M]].$$

其中,

H = Hash函数(如SM3, SHA-3等);

IV = Hash函数的初始向量;


M = HMAC的消息输入 (包括由Hash函数定义的填充位);

Y_i = M 的第 i 个分组, $0 \leq i \leq (L-1)$;

L = M 中的分组数;

b = 每个分组所含的位数, 由所用的Hash函数确定;





四、报文认证与消息认证码

② HMAC

n = Hash码的长度, $b > n$;

K = 密钥; 建议密钥长度 $\geq n$ 。若密钥长度大于 b , 则将密钥作为Hash函数的输入, 来产生一个 n 位的密钥;

K^+ = 在 K 左边填充0后形成标准块, 所得的 b 位结果;

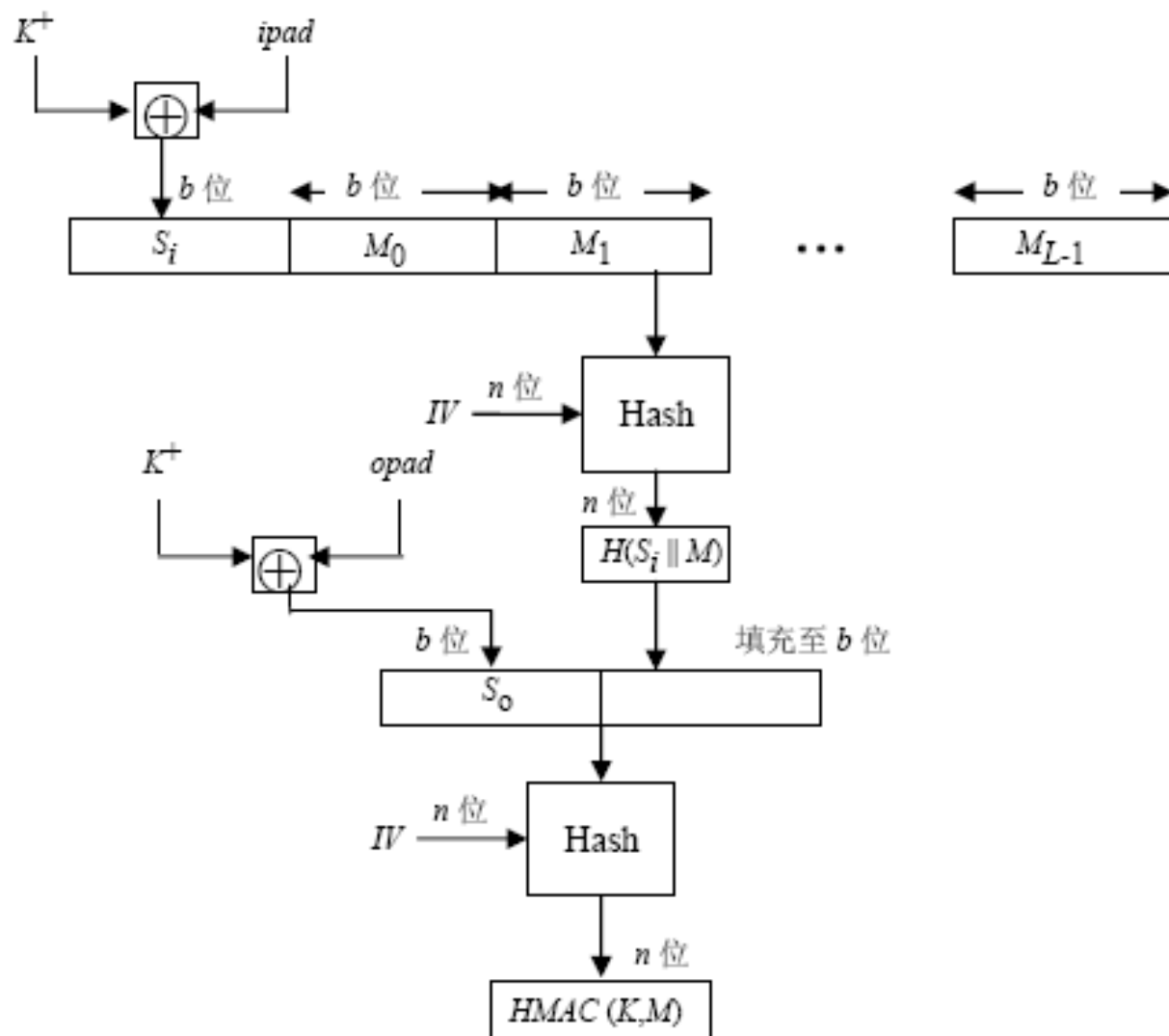
ipad = 00110110 (十六进制数36) 重复 $b/8$ 次的结果;


opad = 01011100 (十六进制数5C) 重复 $b/8$ 次的结果。



四、报文认证与消息认证码

② HMAC






四、报文认证与消息认证码

② HMAC

● HMAC的安全性:

- 在HMAC计算过程中**密钥 K 两次参与计算**，如果 K 是安全的，则伪造HMAC是困难的。
- 在HMAC计算过程中**Hash函数两次参与计算**，如果所用的Hash函数是安全的，则HMAC是安全的。
- 建议HMAC使用SM3或SHA-3等强Hash函数。





四、报文认证与消息认证码

6. 报文的时间性认证


① 序列号

- 发送方在每条报文后附加上序列号，只有在序列号正确时接收方才认为接收到的报文是正确的。由于每一通信方都必须记录与其他各方通信的最后序列号，因此比较麻烦。

② 时间戳

- 发送方在第 i 份报文中加入时间参数 T_i ，接收方只需验证 T_i 的顺序是否合理，便可确认报文的顺序是否正确。
- 可以用日期时间值 $TOD1, TOD2, \dots, TODn$ 。取为年、月、日、时、分、秒即可。 $TODi$ 为发送第 i 份报文时的时间。这种方法要求通信各方的时钟应保持同步。





四、报文认证与消息认证码

6. 报文的时间性认证

③ 随机数/响应

- 每当A要发报文给B时，A先通知B，B动态地产生一个随机数 R_B ，并发送给A。A将 R_B 加入报文中，加密后发给B。B收到报文后解密还原 R_B ，若解密所得 R_B 正确，便确认报文的顺序是正确的。
- 这种方法需要在传输报文之前先交互随机数，适应于双工通信。





认证的实际应用

- Kerberos
- X.509
- 公钥基础设施PKI





Kerberos认证系统

- 项目背景
 - Kerberos是MIT1985年开始的Athena计划中的一部分，是为UNIX TCP/IP网络设计的三方认证协议。
 - 网络上的Kerberos服务设施作为信赖的仲裁者。Kerberos提供安全的网络认证，允许一个用户访问网络上的不同机器。
 - Kerberos基于对称密码技术。
 - Kerberos第4版是“最初的”Kerberos，还在广泛使用。第5版弥补了第4版中存在的某些安全漏洞，并已作为Internet标准草案发布（RFC 1510）。





Kerberos认证系统

- 问题的提出
 - 在一个公开的分布式环境中，工作站上的用户希望访问分布在网络中服务器上的服务。服务提供者则希望服务器能限制授权用户的访问，并能对服务请求进行鉴别。
 - 因此，Kerberos不是建立一个精细的鉴别协议，而是提供一个集中的鉴别服务器，功能是实现服务器与用户间的相互鉴别。





Kerberos认证系统

- Kerberos的设计目标
 - Kerberos假定一个分布的客户服务器结构，并使用一个或多个Kerberos服务器来提供鉴别服务。并期望满足下述需求：安全，可靠，透明，可伸缩。
 - 为了支持这些需求，Kerberos的总体方案是使用一个协议来提供可信的第三方鉴别服务。客户和服务器的信任Kerberos能仲裁它们之间的相互鉴别，从这个意义上说它是可信的。假定Kerberos协议已经设计好，如果Kerberos服务器本身是安全的，那么鉴别服务就是安全的。





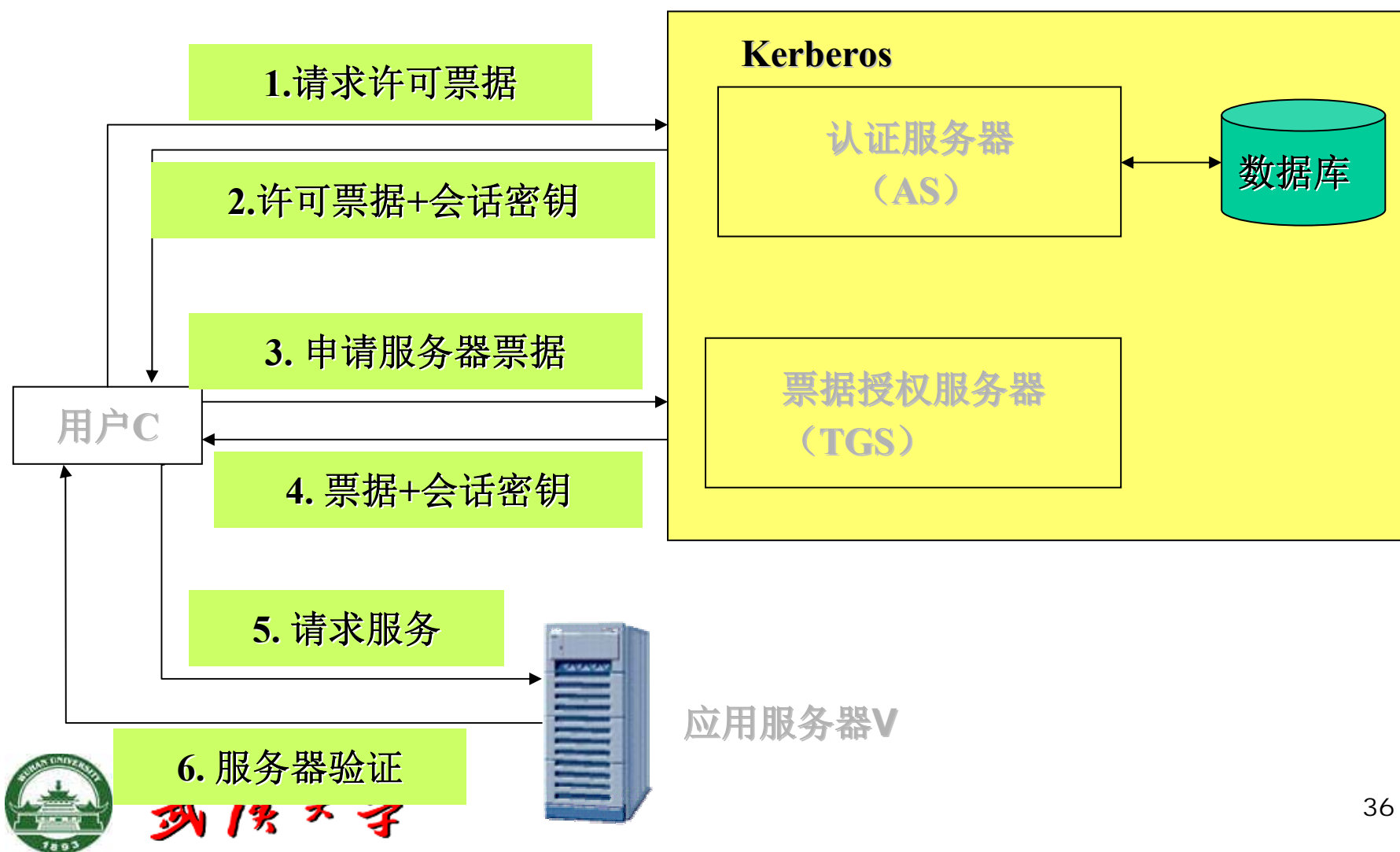
Kerberos认证系统

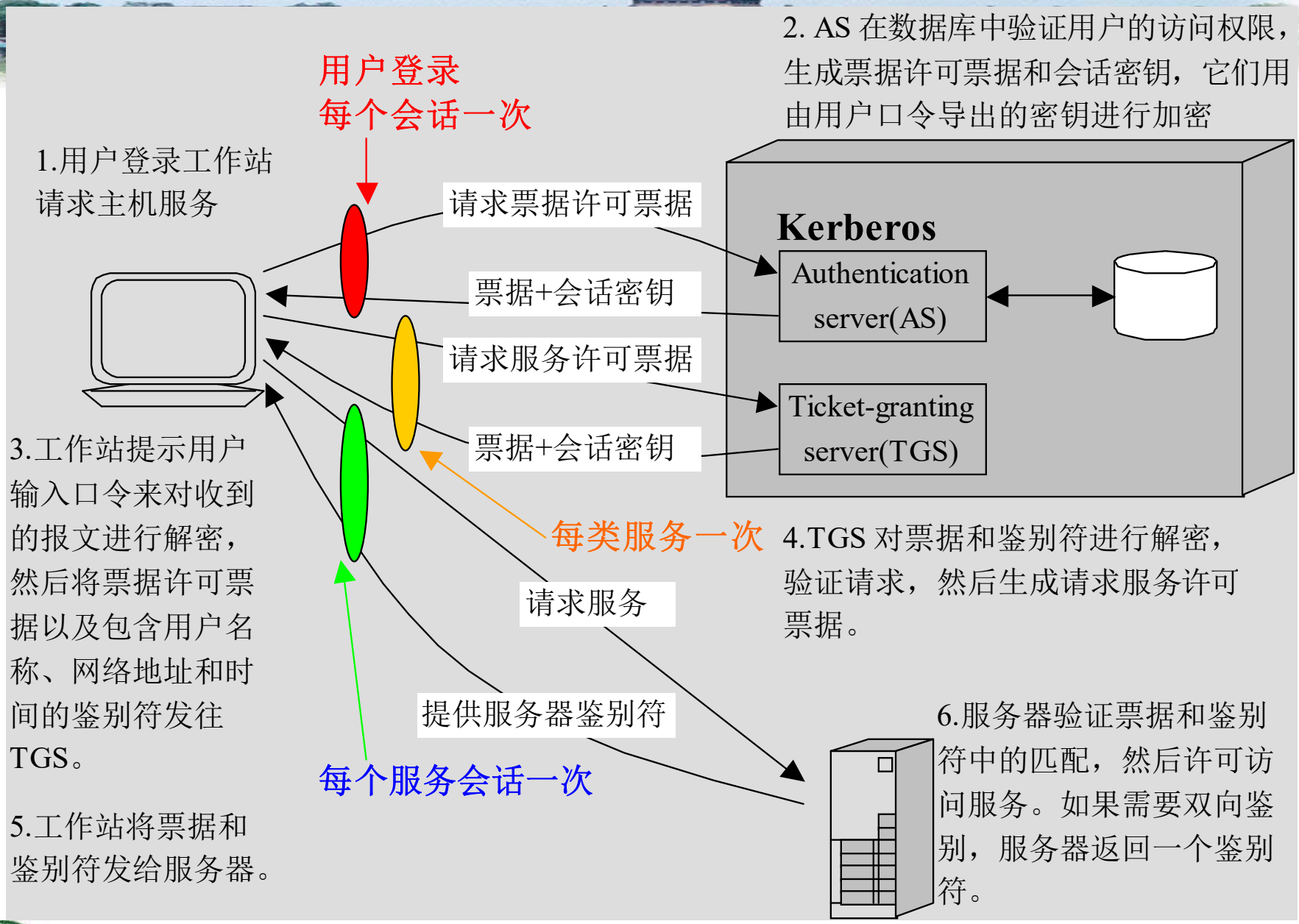
- Kerberos支持在分布式系统中实现认证
 - Kerberos服务器向用户提供一种称为票据的已认证的令牌，用户利用票据向应用软件提出请求。
 - 票据是不能伪造、不能重放、已认证的对象
 - 票据是一种用户可以获得的用于命名一个用户或一种服务的加密数据结构，其中保护时间值和一些控制信息





Kerberos认证系统







Kerberos认证系统

- 优点
 - 网络中无口令信息的通信
 - 使用加密提供保密性，防止欺骗
 - 有效的有效期
 - 时间戳防止重放攻击
 - 相互认证





Kerberos认证系统

- 缺点
 - 要求一个可信任的票据授权服务器连续可用
 - 服务器的真实性要求在票据授权服务器与每个服务器之间保持一种信任关系
 - 要求实时传输
 - 一个被安装破坏的工作站可存储用户口令，并在稍后重放该口令
 - 口令猜测攻击





Kerberos认证系统

- Kerberos 5 ——协议的改进模型
 - 消除认证协议对安全时间服务的依赖性
 - 更好地防止重放攻击
 - 提高口令猜测的复杂度
 - 简化域间认证
 - 提供效率
 - 使用临时交互号nonce





谢 谢！



武汉大学