



哈爾濱工業大學(深圳)  
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

# 通 信 安 全

## L7—认证技术



- 教师：崔爱娇
- 编号：ELEC3019
- 学时：32学时



## 认证技术

认证技术基本知识

口令认证

数字证书认证

生物特征认证

## 认证技术

认证技术基本知识

口令认证

数字证书认证

生物特征认证

# 生活中的认证

## ➤ 入学查看学生的入学通知书



## ➤ 微信支付输入密码



## ➤ 通关检验输入指纹





# 认证的目的

## ➤ 问题的提出

身份欺诈

## ➤ 认证的需求

某成员（声称者）提交一个主体的身份并声称他是那个主体

## ➤ 认证目的

使别的成员（验证者）获得对声称者所声称的事实的信任。



# 认证（authentication）的作用

确认实体（或消息）是它所声明的。

认证是最重要的安全服务之一。认证服务提供了关于某个实体身份的保证。（所有其它的安全服务都依赖于该服务）

认证可以对抗假冒攻击的危险。



# 认证的两种情形

**身份认证**：某一实体确信与之打交道的实体正式所需要的实体。只是简单的认证实体本身的身份，不会和实体想要进行何种活动相联系。

**消息认证**：鉴定某个指定的数据是否来源于某个特定的实体。不是孤立的鉴别一个实体，也不是为了允许实体执行下一步的操作而认证它的身份，而是为了确定被认证的实体与一些特定数据项有着静态的不可分割的联系。

## 身份认证的分类

**单向认证**：通信双方中只有一方向另一方进行认证。

**双向认证**：通信双方相互进行认证。

# 身份认证系统的简介

P



出示证件的人。示证者P  
(prover) 声称者 (claimant)

V



检验声称者提出的证件的正确性  
和合法性。验证者V (verifier)

P ??



安全的身份识别协议至少满足以下两个条件：

1. 示证者P能向验证者V证明他的确是P。
2. 在示证者P向验证者V证明他的身份后，验证者V没有获得任何有用的信息，V不能模仿P向第三方证明他是P。





# 身份认证的分类

所知：密码、口令（散列口令、口令更改）等。

所有：身份证、护密钥盘、usb key等。

所是：指纹、笔迹、声音、虹膜、DNA。

## 认证技术

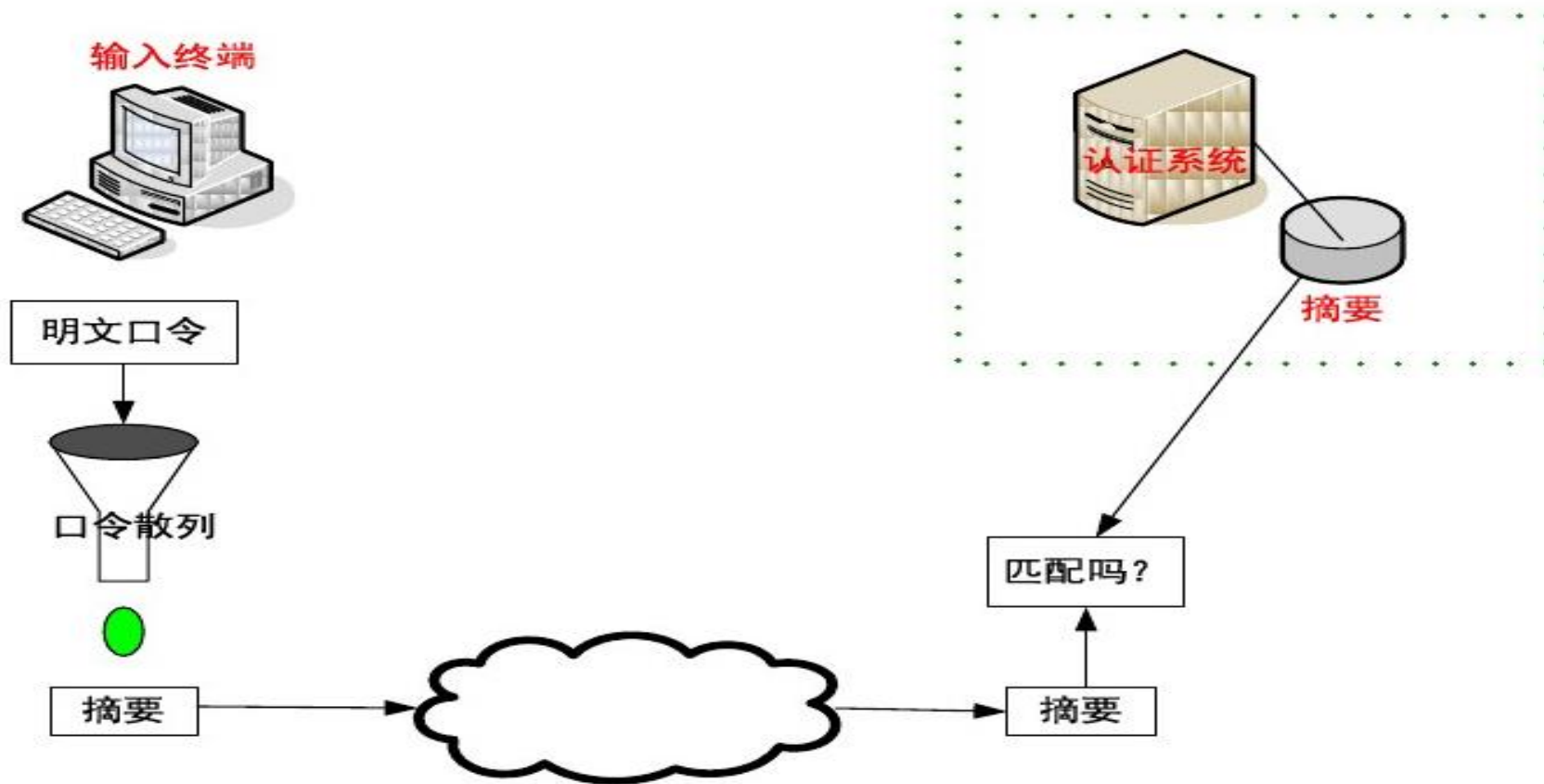
认证技术基本知识

口令认证

数字证书认证

生物特征认证

# 散列口令



- 系统不存储明文
- 明文不在网上传输
- 根据摘要无法推出口令

- 重放攻击
- 穷举攻击



# 重放攻击及作用



重放攻击(Replay Attacks)又称重播攻击、回放攻击，是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。

- 巧妙实现了信息注入，不需要了解、分析通信协议；
- 实现了流量攻击，即通过额外增加的数据流影响正常数据流的传输时延，耗用通信链路的带宽；
- 实现了可能的差错攻击，一般的链路通信协议都实现流量控制功能，通过数据流重放，很可能会干扰正常的流量控制窗口和数据帧的发送(应答)序列号，导致数据重传或误收。



# 防御方案

👍 该方法优点是认证双方不需要时间同步，双方记住使用过的随机数，如发现报文中以前使用过的随机数，就认为是重放攻击。**(1)加随机数。**

👎 缺点是需要额外保存使用过的随机数，若记录的时间段较长，则保存和查询的开销较大。

👍 该方法优点是不用额外保存其他信息。**(2)加时间戳。**

👎 缺点是认证双方需要准确的时间同步，同步越好，受攻击的可能性就越小。但当系统很庞大，跨越的区域较广时，要做到精确的时间同步并不是很容易。

就是双方在报文中添加一个逐步递增的整数，只要接收到一个不连续的流水号报文(太大或太小)，就认定有重放威胁。**(3)加流水号**

👍 该方法优点是不需要时间同步，保存的信息量比随机数方式小。

👎 缺点是一旦攻击者对报文解密成功，就可以获得流水号，从而每次将流水号递增欺骗认证端。



# 防御方案

- 在实际中，常将方法(1)和方法(2)组合使用，这样就只需保存某个很短时间段内的所有随机数，而且时间戳的同步也不需要太精确。
- 对付重放攻击除了使用以上方法外，还可以使用挑战一应答机制和一次性口令机制，而且后面两种方法在实际中使用得更广泛。



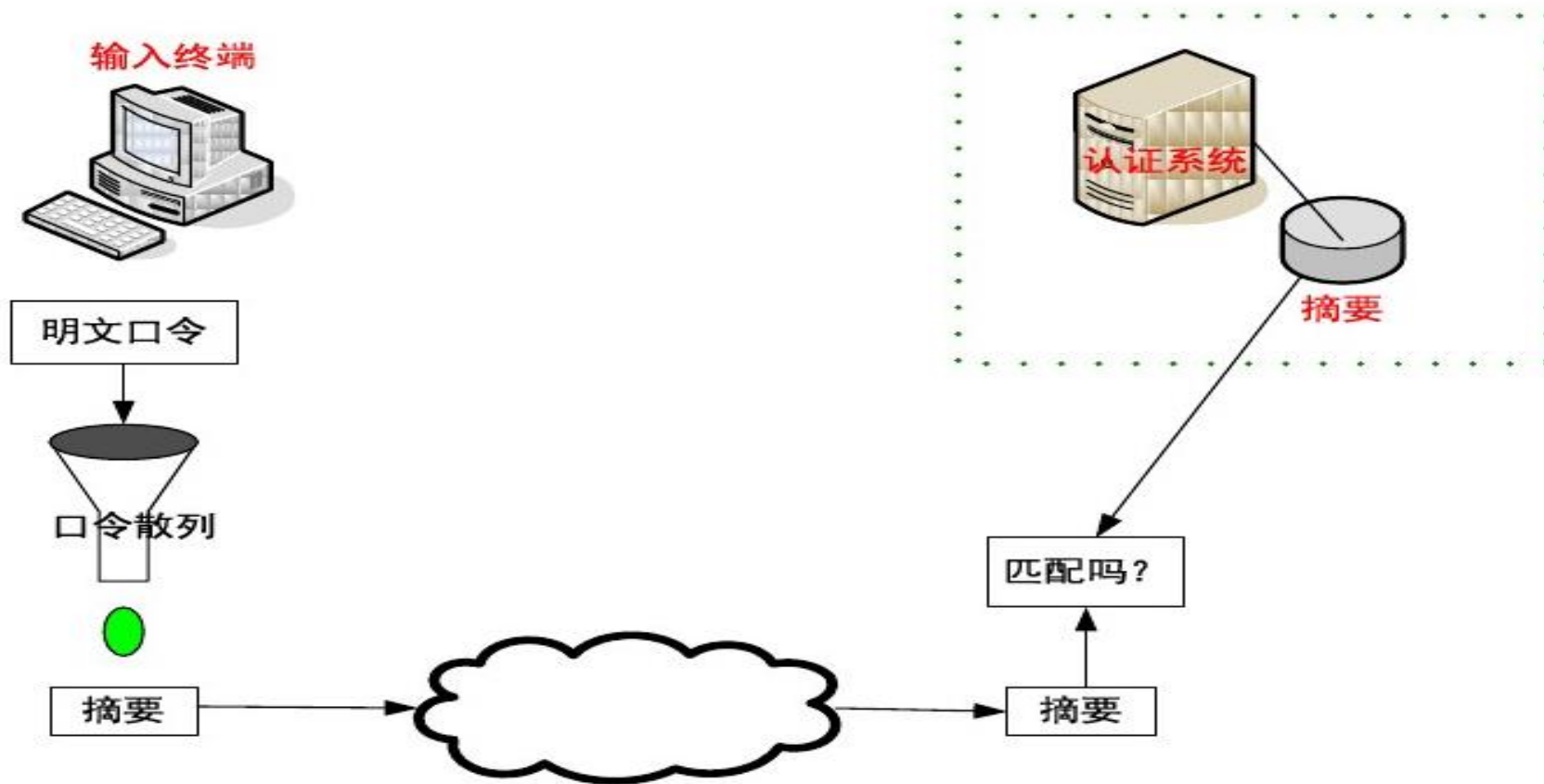
# 穷举攻击

- 从理论上讲，可以尝试所有的密钥穷举攻击的代价与密钥大小成正比
- 密码算法可以通过增大密钥位数或加大解密（加密）算法的复杂性来对抗穷举攻击

密钥长度（位）	密钥数目	尝试时间（1次/微秒）	尝试时间（ $10^6$ 次/微秒）
32	$2^{32}=4.3\times 10^9$	35.8分	2.15毫秒
56	$2^{56}=7.2\times 10^{16}$	1142年	10.01小时
128	$2^{128}=3.4\times 10^{38}$	$5.4\times 10^{24}$ 年	$5.4\times 10^{18}$ 年
168	$2^{168}=3.7\times 10^{50}$	$5.9\times 10^{36}$ 年	$5.9\times 10^{30}$ 年
26个字母排列	$26! =4\times 10^{26}$	$6.4\times 10^{12}$ 年	$6.4\times 10^6$ 年

从表中我们可以发现，当密钥长度达到128位以上时，以目前的资源来说，穷举攻击将不成功。

# 散列口令

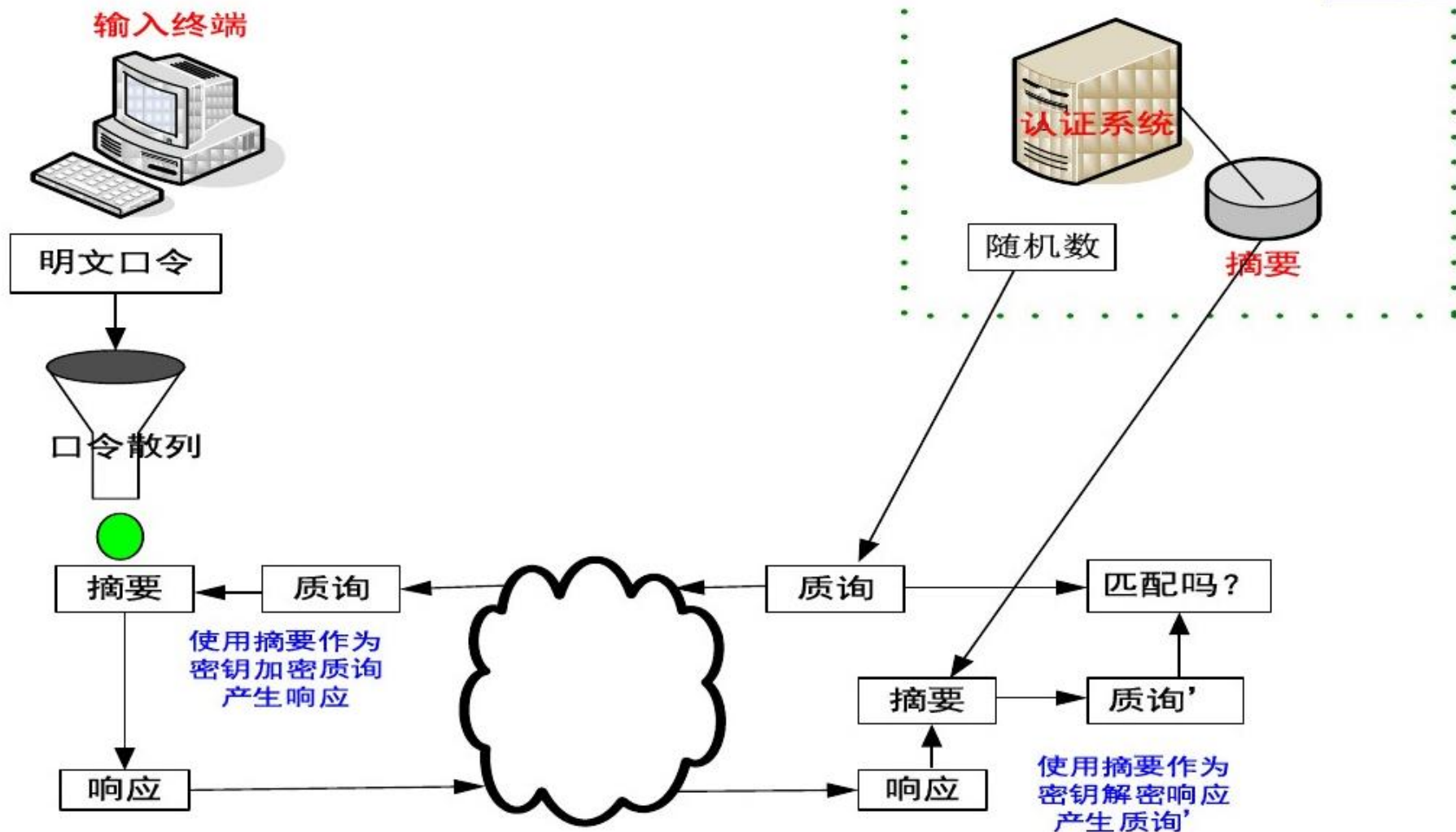


- 系统不存储明文
- 明文不在网上传输
- 根据摘要无法推出口令

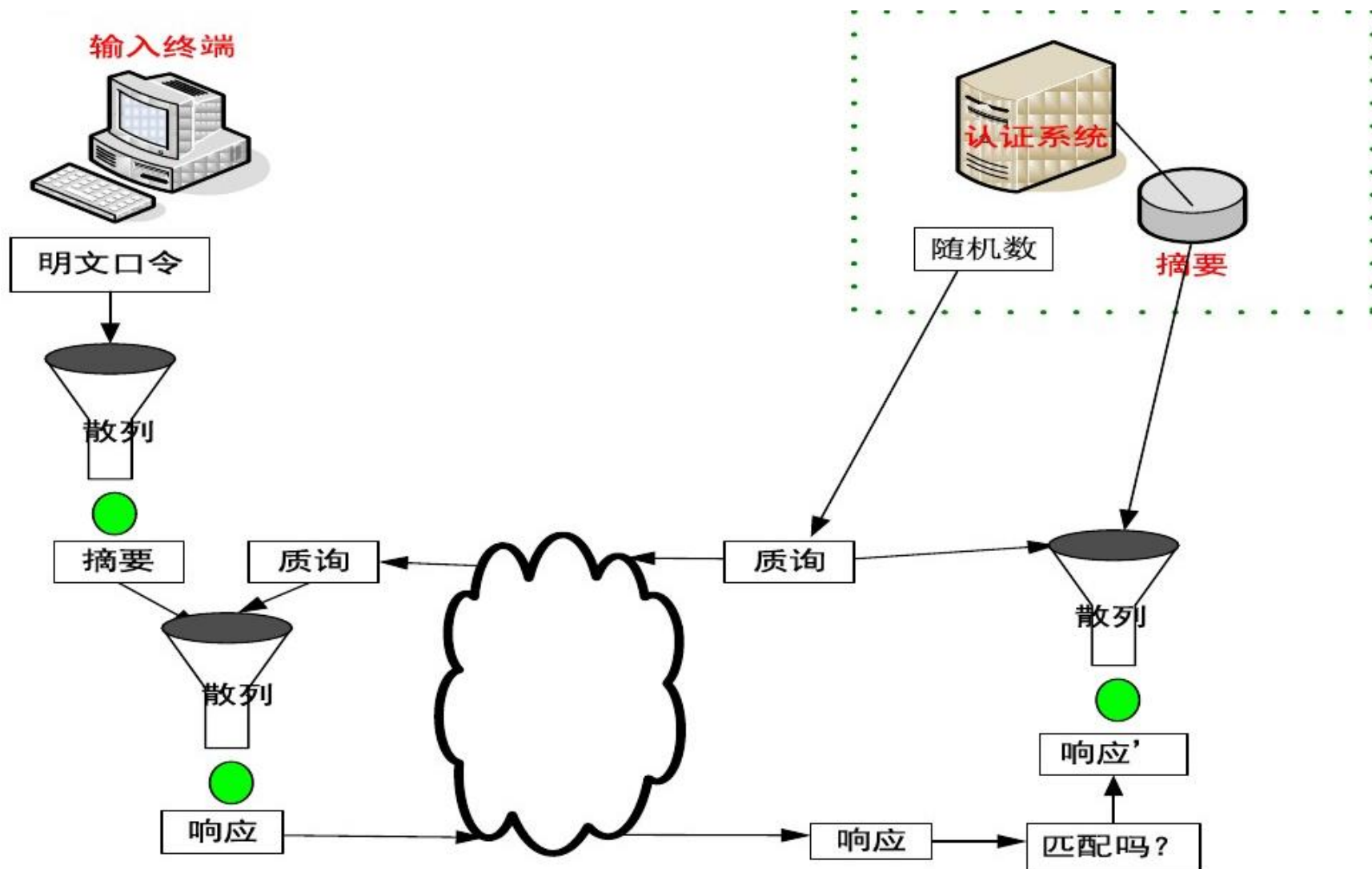
- 重放攻击
- 穷举攻击



# 改进方案（一）



# 改进方案（二）

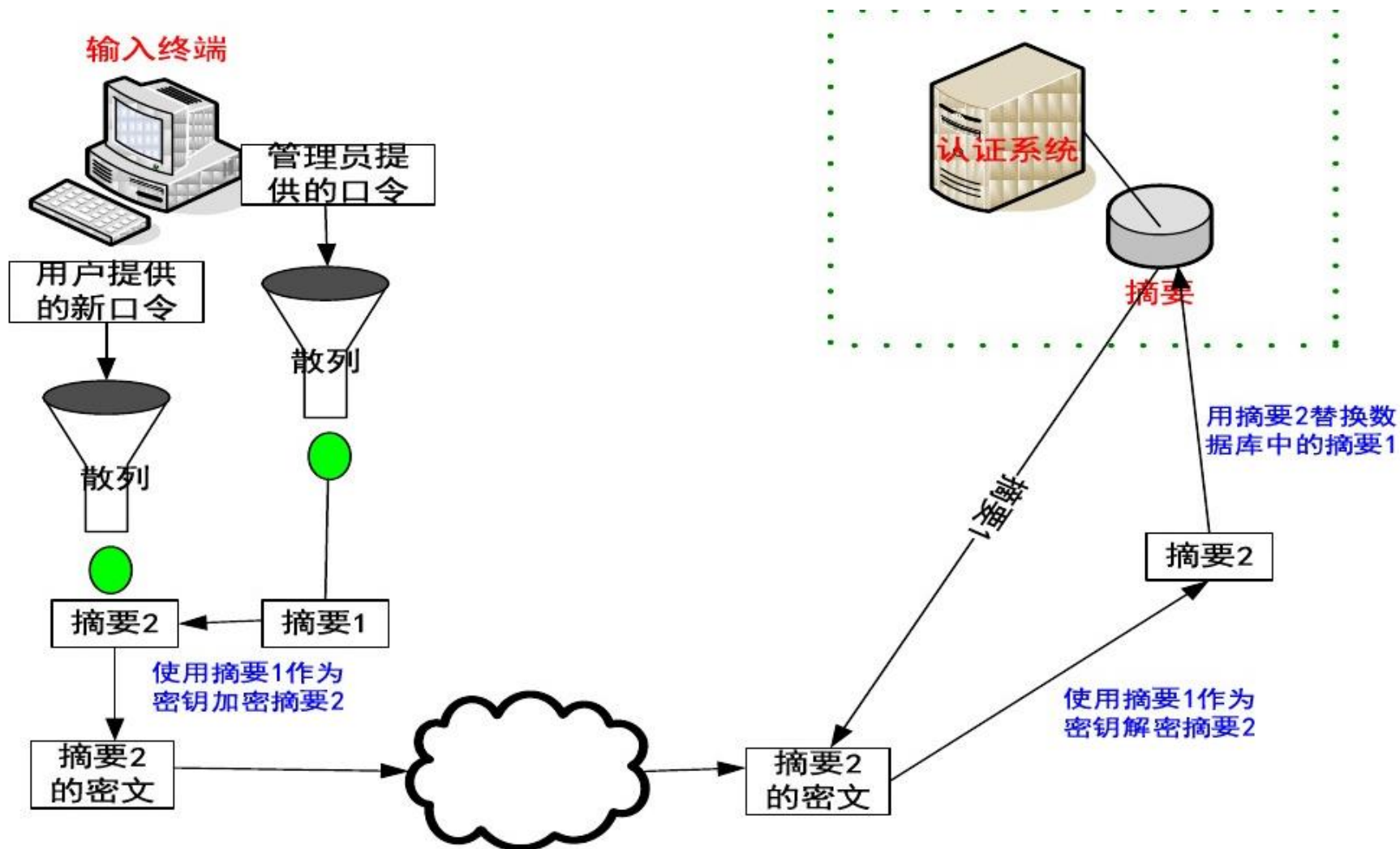




# 口令更新

- 对于大部分系统而言，初始化时，系统管理员给每个用户指定一个通过散列计算出来的临时口令，认证数据库中保存临时口令的摘要。
- 管理员通过某些带外的方式，如邮件或者电话，告诉用户的口令。
- 用户口令应定期修改

# 口令更新的实现





# 口令小结

- 口令是当前最常用的认证方式。
- 现代口令系统以质询/响应系统和散列密码算法为基础。
  - 1) 明文口令不存储在任何地方
  - 2) 系统管理员不知道终端用户口令。
- 用户第一次登入时需要更改口令
- 口令事实上是最昂贵的认证方式之一



# 认证令牌

- 认证令牌是简单口令最常见的替代品。
- 认证令牌就是为每一次认证产生一个用于认证的新值的设备。
- 认证令牌一版是由一个处理器、一个液晶显示屏（LCD）和一块电池组成的。
- 每个令牌都用称为种子唯一值的编程，种子可确保每个令牌产生唯一的输出代码。
- 认证服务器必须知道每个令牌的编程种子数。
- 令牌认证是双因子认证（口令是单因子）

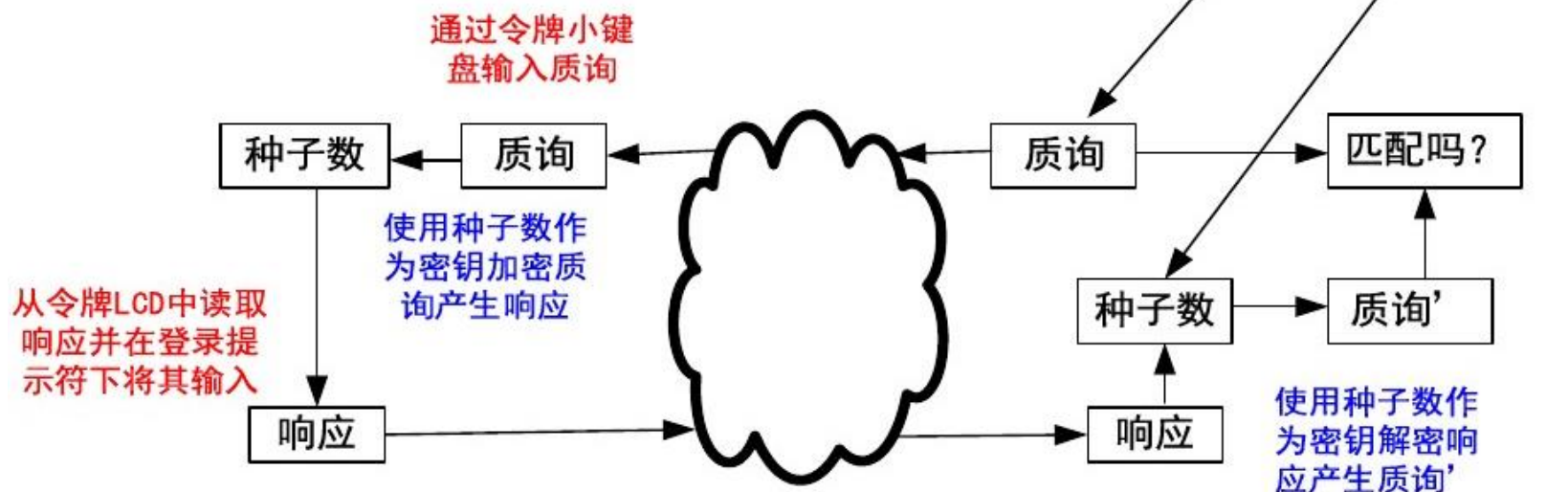
质询/响应令牌

时间令牌

# 质询/响应令牌



质询/响应  
令牌





# 质询/响应令牌



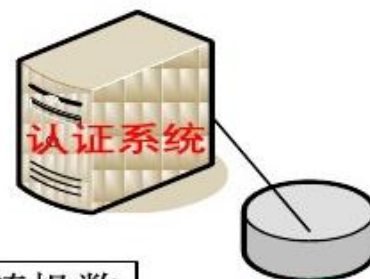
质询/响应  
令牌

通过令牌小键  
盘输入质询

按需要截取适  
当长度的字符  
串作为响应

使用种子数作为  
密钥加密质询

从令牌LCD中读取  
响应并在登录提  
示符下将其输入



随机数

种子数

使用种子数运行  
相同的加密算法

使用相同方法  
截取加密结果

响应'

匹配吗?

种子数

质询

质询

种子数

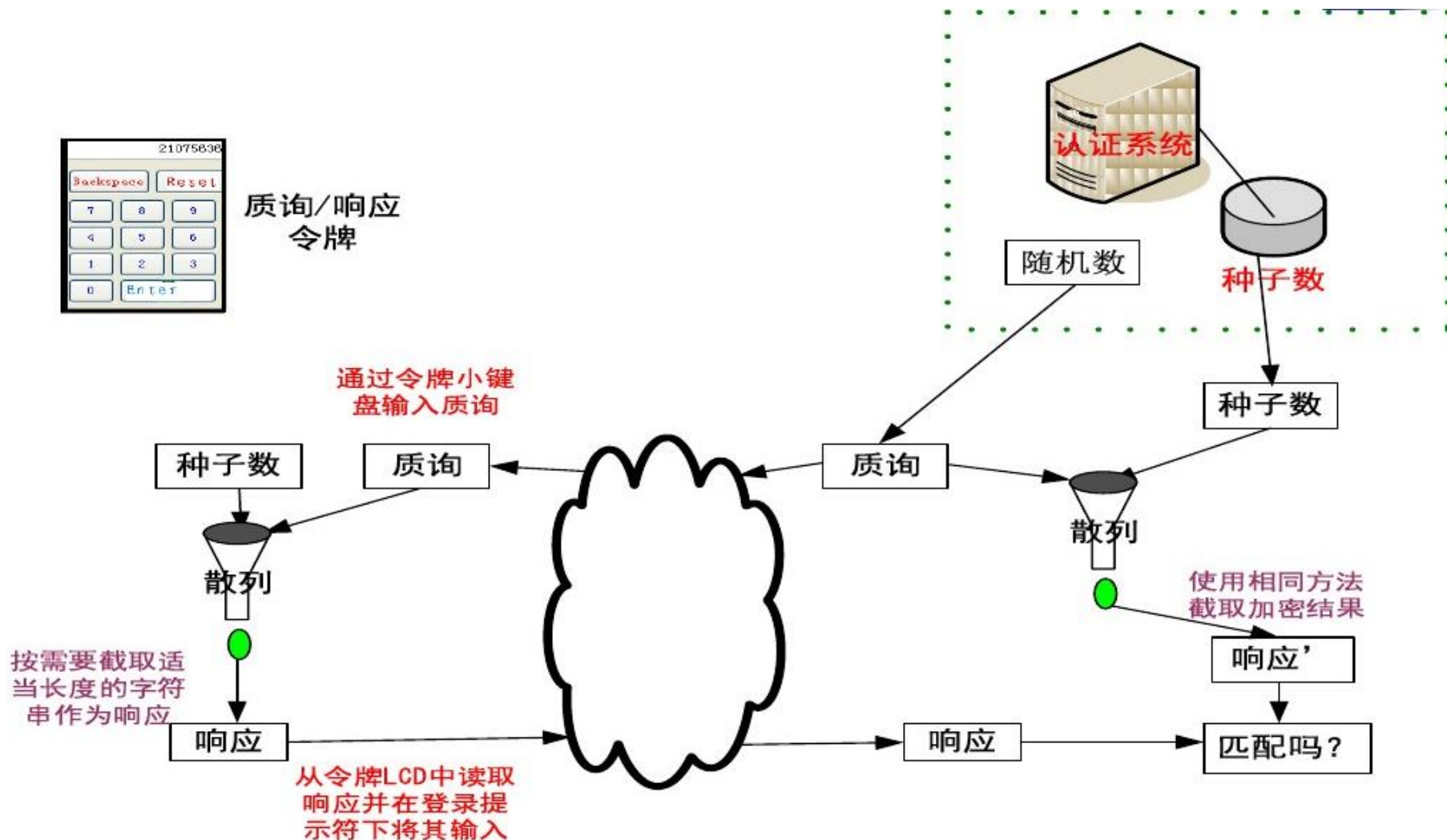
响应

响应

响应'



# 质询/响应令牌





# 时间令牌

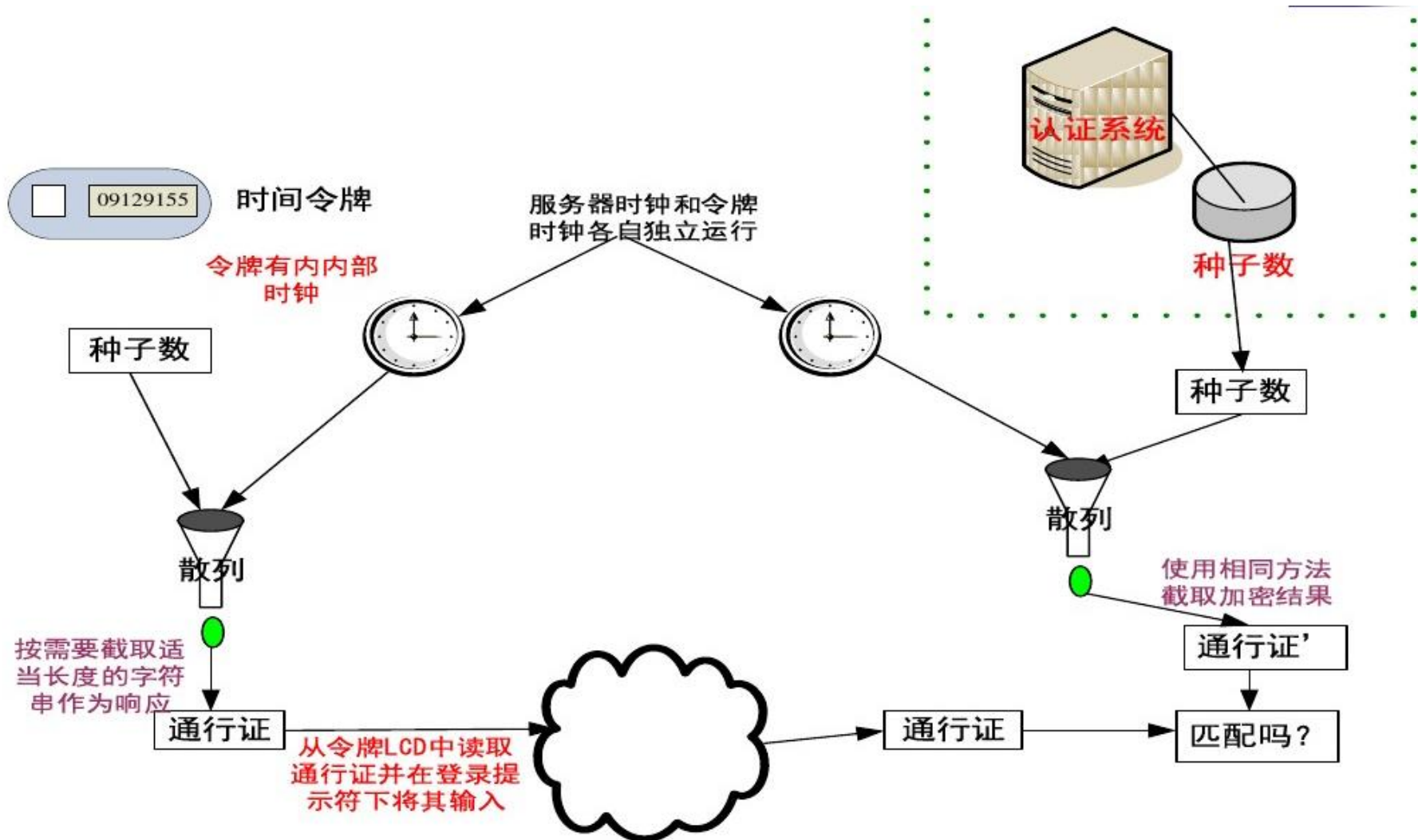
质询/响应令牌的缺陷：

用户认证必须准确的读取两个不同值（质询和响应）  
正确的输入三个不一样的数值（PIN、质询、响应）



时间令牌是更容易的令牌

# 时间令牌的实现





# 时钟的同步

- 令牌时钟在生产过程时对其初始化并植入了校对因子。
- 令牌每60秒产生一个新的通行字。
- 认证服务器通过以服务器时钟为中心点，加上或减去几分钟的滑动窗口来尝试和查找认证通行码，同时调整时间偏移量。
- 如果通行码在内部窗口未获匹配，则在大窗口内查找，若匹配，用户需再输入一次确保用户不是伪造的，再次匹配，认证通过并同时调整时间偏移量，否则，认证不通过。



# 认证令牌小结

- 认证令牌主要有两种类型：质询/响应和时间令牌。
- 认证令牌引入了双因素认证的概念。
- 质询/响应令牌看起来很像一个小计算器，有一个液晶显示屏（LCD）和一个小键盘。用户通过小键盘输入质询和PIN。令牌计算出响应并显示在液晶显示屏上，用户把响应输入到登陆提示符下。
- 本质上，质询/响应令牌对种子数和质询一起进行散列运算生成一个伪随机数，然后截取该数的部分字符显示在液晶显示屏上。
- 质询/响应令牌和基于口令的质询/响应方案不同在于它需要对产生的伪随机数进行截取。



# 认证令牌小结

- 时间令牌看起来好像一个小钥匙装饰物，只有液晶显示屏而没有小键盘。用户只要在登录提示符下输入PIN，紧接着输入令牌产生的伪随机数即可。
- 实质上，时间令牌维护着一个实时时钟，它的输出与种子数一起参加散列运算产生一个伪随机数，然后截取部分字符显示在液晶显示屏上。
- 时间令牌关键在于时钟同步、校对、窗口设置。
- 还有一种软件实现的令牌，运行在PC上，手机上

## 认证技术

认证技术基本知识

口令认证

数字证书认证

生物特征认证



# 哈希算法

- 哈希是一种加密算法，也称为散列函数或杂凑函数。
- 哈希函数是一个公开函数，可以将任意长度的消息 $M$ 映射成为一个长度较短且长度固定的值 $H(M)$ ，称 $H(M)$ 为哈希值、散列值（Hash Value）、杂凑值或者消息摘要。
- 它是一种单向密码体制，即一个从明文到密文的不可逆映射，只有加密过程，没有解密过程。

MD4, MD5

SHA家族





# 哈希的特点

易压缩：对于任意大小的输入 $x$ ，Hash值的长度很小，在实际应用中，函数 $H$ 产生的Hash值其长度是固定的。

易计算：对于任意给定的消息，计算其Hash值比较容易。


单向性：对于给定的Hash值，要找到使得在计算上是不可行的，即求Hash的逆很困难。在给定某个哈希函数 $H$ 和哈希值 $H(M)$ 的情况下，得出 $M$ 在计算上是不可行的。即从哈希输出无法倒推输入的原始数值。这是哈希函数安全性的基础。

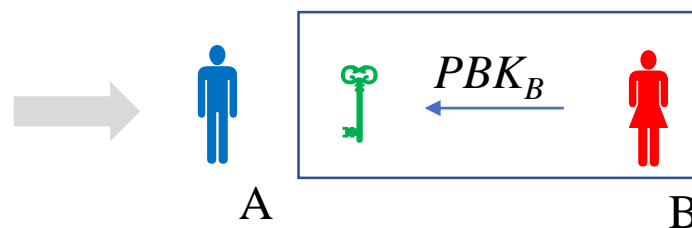
抗碰撞性：理想的Hash函数是无碰撞的，但在实际算法的设计中很难做到这一点。

高灵敏性：这是从比特位角度出发的，指的是1比特位的输入变化会造成1/2的比特位发生变化。消息 $M$ 的任何改变都会导致哈希值 $H(M)$ 发生改变。即如果输入有微小不同，哈希运算后的输出一定不同。


# 数字证书

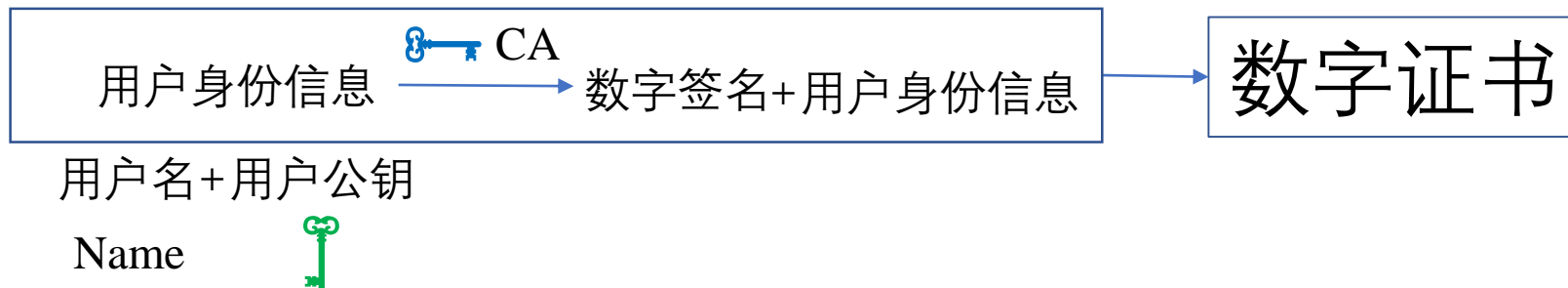
A如何确定给自己回信息的是B??

  
C 把A保存的B的公钥偷偷换成自己的，并冒用B的名义给A发信息



A只要能确定自己持有的公钥到底是不是B的

 数字证书:就是一个人或者组织在网络世界中的身份证。由发证机关证书管理机构 (CA: Certificate authority)





# 数字证书

**证书发布机构**：这个证书是哪个证书中心（certificate authority，简称CA）发布的。

**证书有效期**：证书的有效期限，过期作废。

**公钥**：用来对消息进行加密解密的，是很长的一串数字。

**证书所有者**：这个证书是发布给谁的，一般是某人或某公司、机构的名称、公司网址。

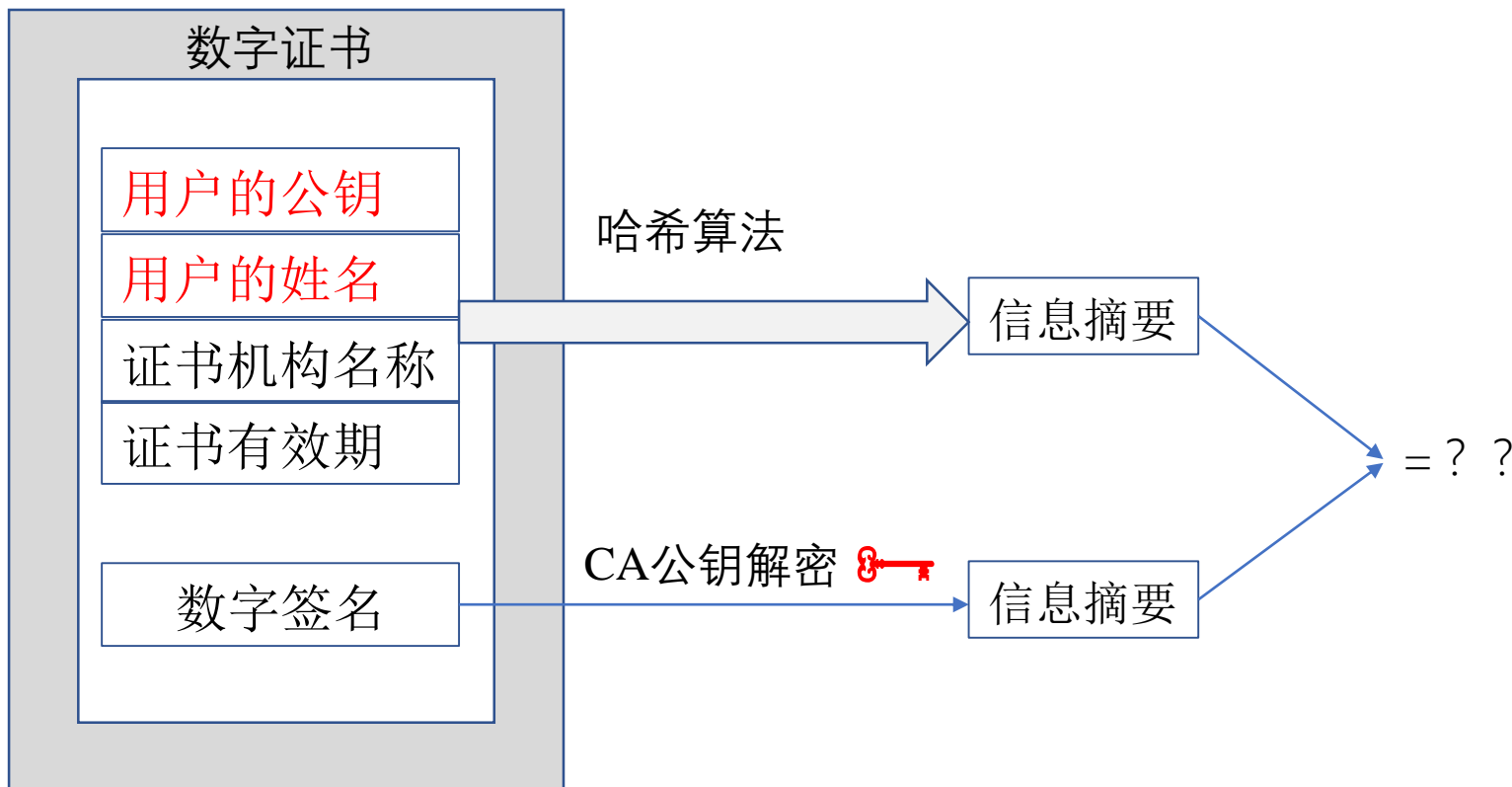
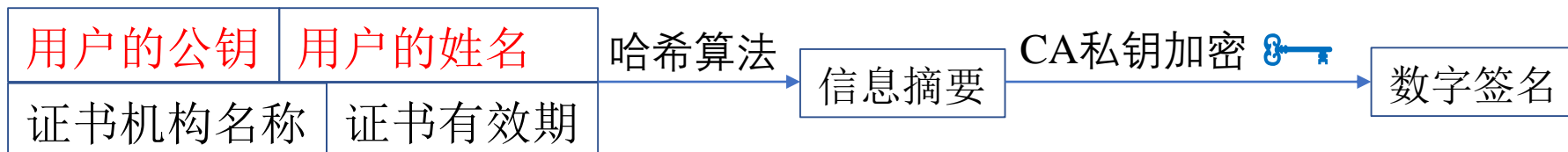
**签名所使用的算法**：指数字签名所使用的加密算法

这样就可以使用证书发布机构的证书里面的公钥，根据这个算法对指纹进行解密。指纹的加密结果就是数字签名

**指纹以及指纹算法**：保证证书的完整性。其原理就是在发布证书时，发布者根据指纹算法(一个hash算法)计算整个证书的hash值(指纹)并和证书放在一起；使用者在打开证书时，自己也根据指纹算法计算一下证书的hash值(指纹)，如果二者匹配，就说明证书没有被修改过。



# 数字证书的生成



## 认证技术

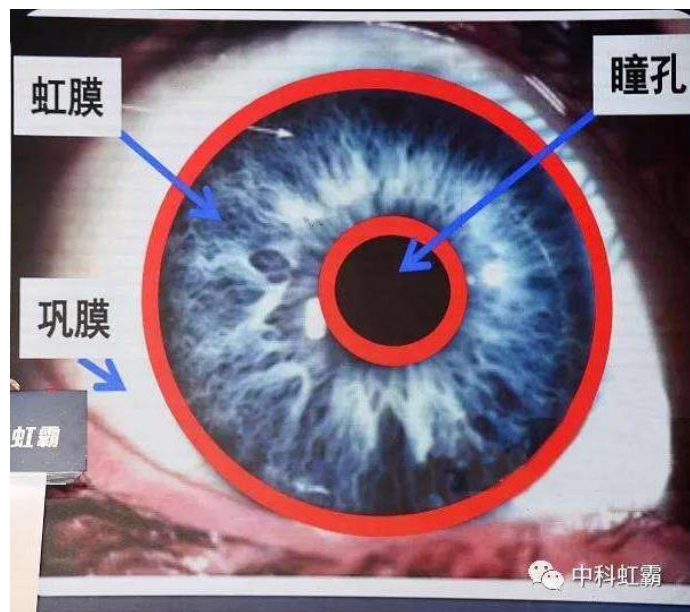
认证技术基本知识

口令认证

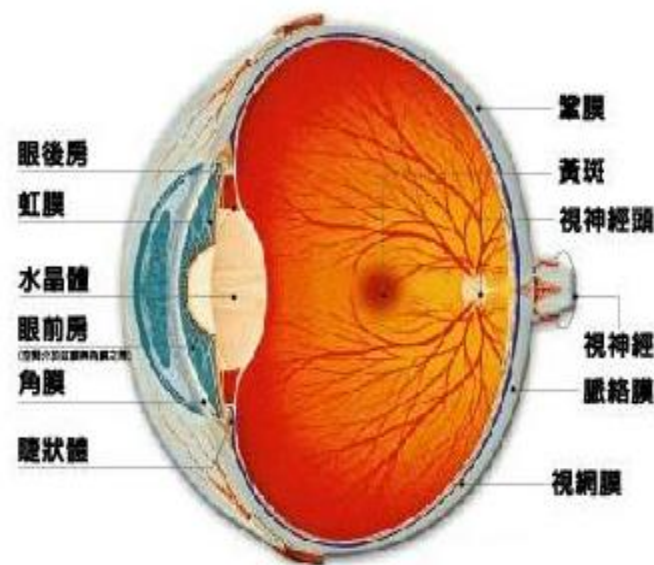
数字证书认证

生物特征认证

# 生物特征认证

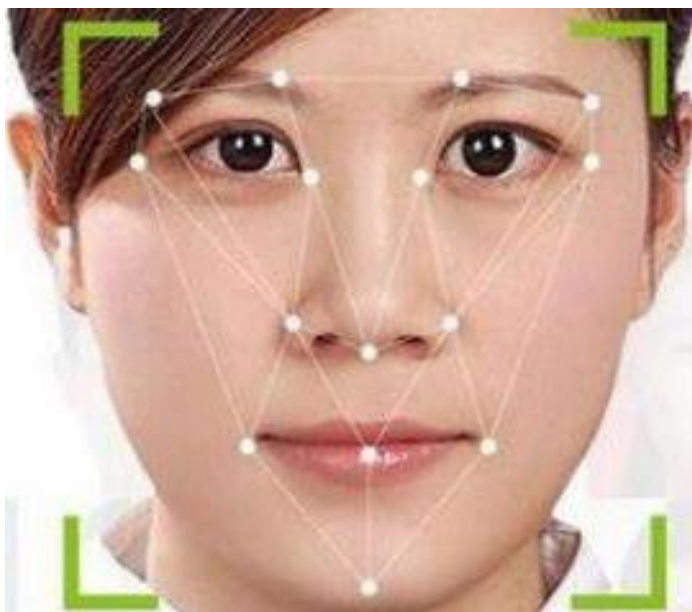


虹膜识别技术（眼睛中瞳孔内的织物状的各色环状物）



视网膜识别技术（激光照射眼球的背面以获得视网膜特征）

# 生物特征认证



面部识别技术



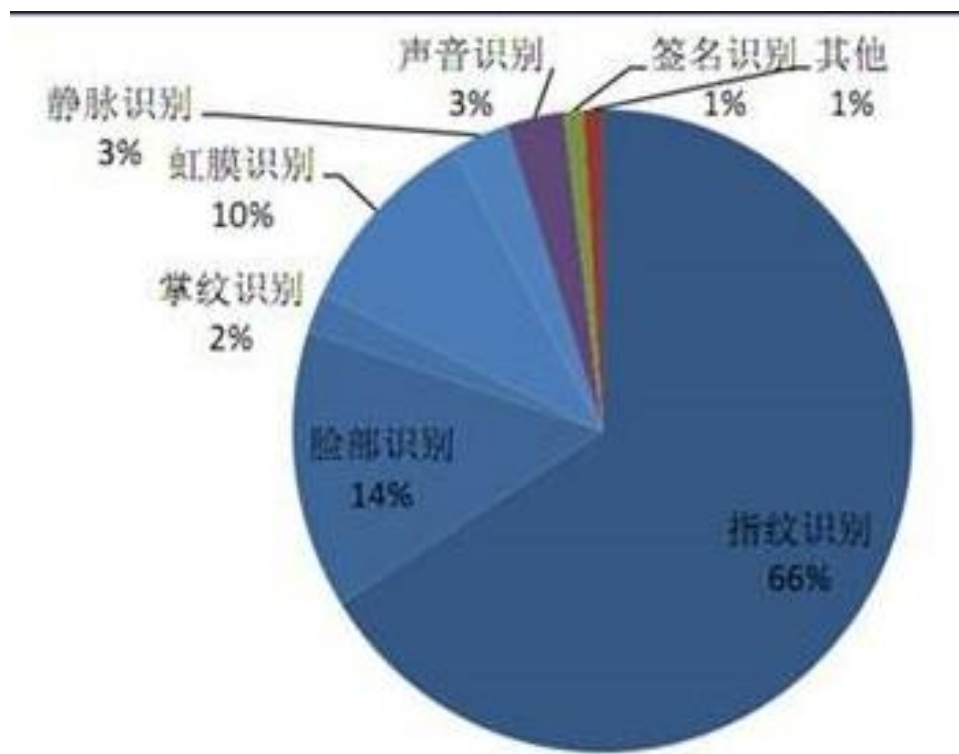
声音识别技术



# 生物特征认证



指纹识别技术



生物识别市场份额





# 生物特征数据

- 生物统计学用于测定用户的一些物理特征。
- 系统在用户每次出示生物特征是采集到的特征数据时不同的。
- 生物认证并不是真正的匹配。
- 系统没有生物特征的完整记录，而只拥有一些典型特征数据。
- 生物认证的关键技术在于生物特征的提取和匹配。



# 两个重要性能指标

➤ 错误接受率（False Accept Ratio, FAR）：衡量用户本应该遭到拒绝却被系统接受的可能性。

➤ 错误拒绝率（False Reject Ratio, FRR）：衡量用户本应该被系统接受却遭到拒绝的可能性。



# 生物特征的优点

➤ 易用的生物特征的解决方案:

一对一匹配, 一对多匹配

➤ 基于安全的生物特征解决方案。

双因子认证, 3因子认证

# 指纹一对多匹配举例



登记



验证

① 输入ID

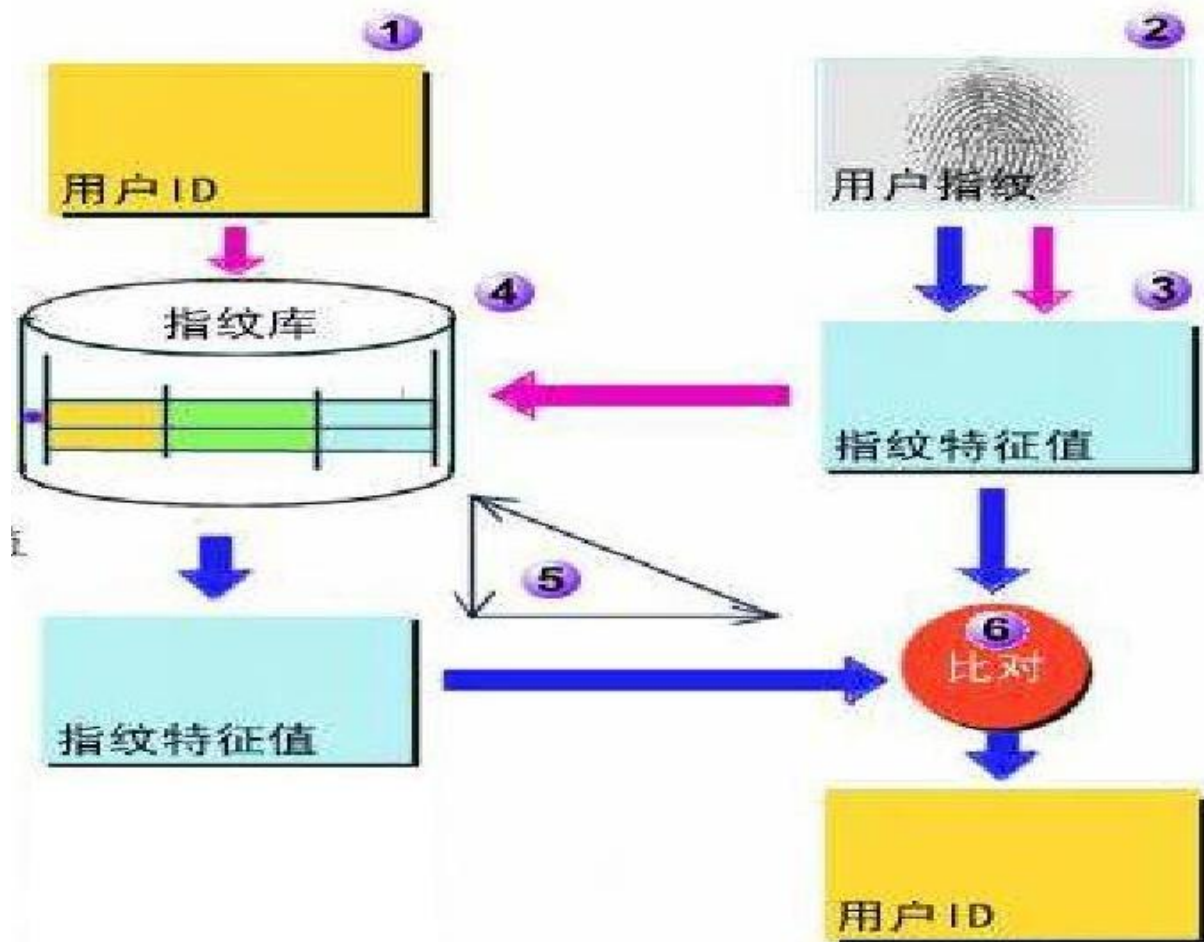
② 出示指纹

③ 计算特征值

④ 保存ID与特征值

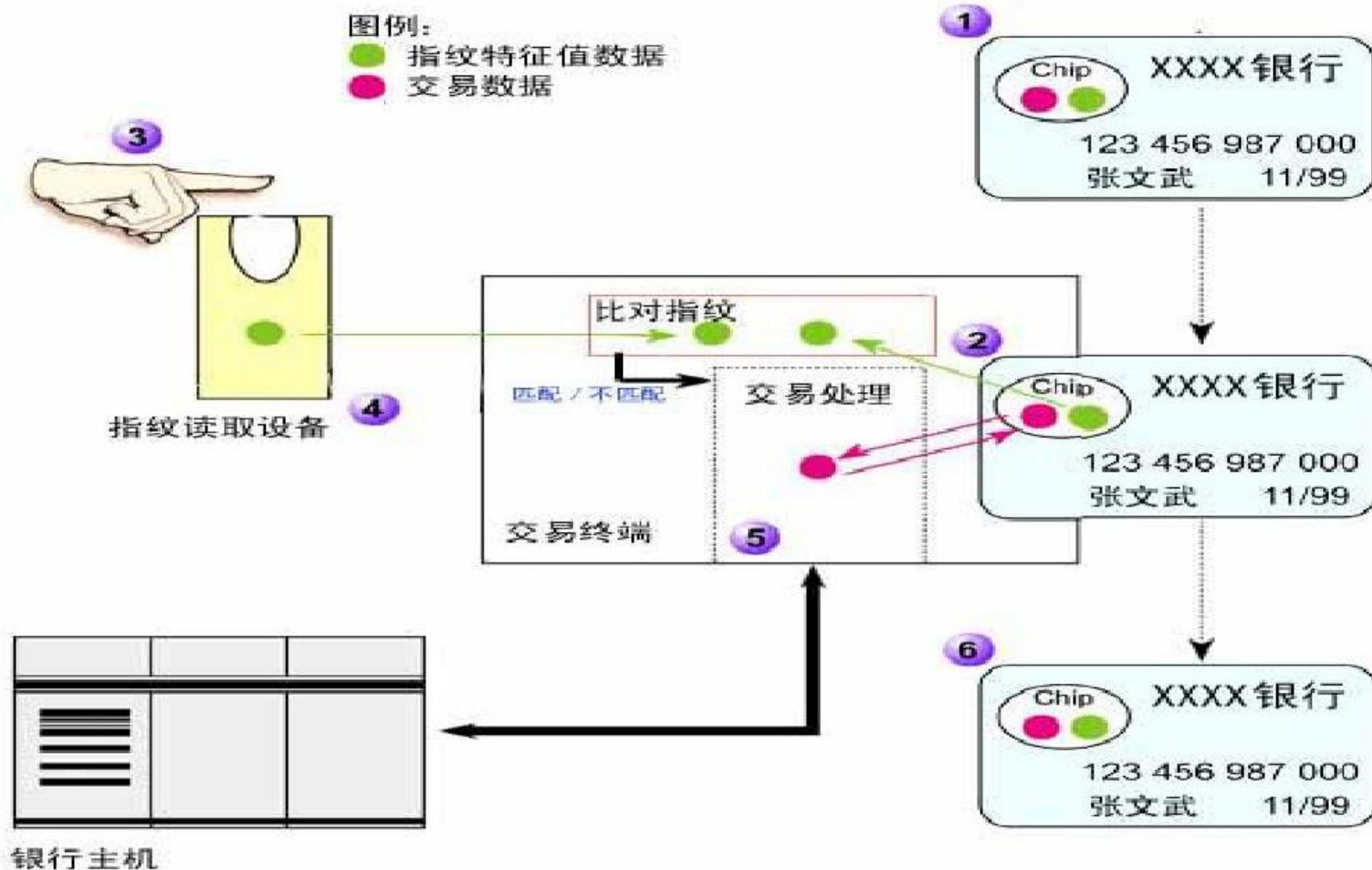
⑤ 逐一比对

⑥ 匹配时输出ID



一对多指纹登记与辨识系统示意图

# 指纹应用举例



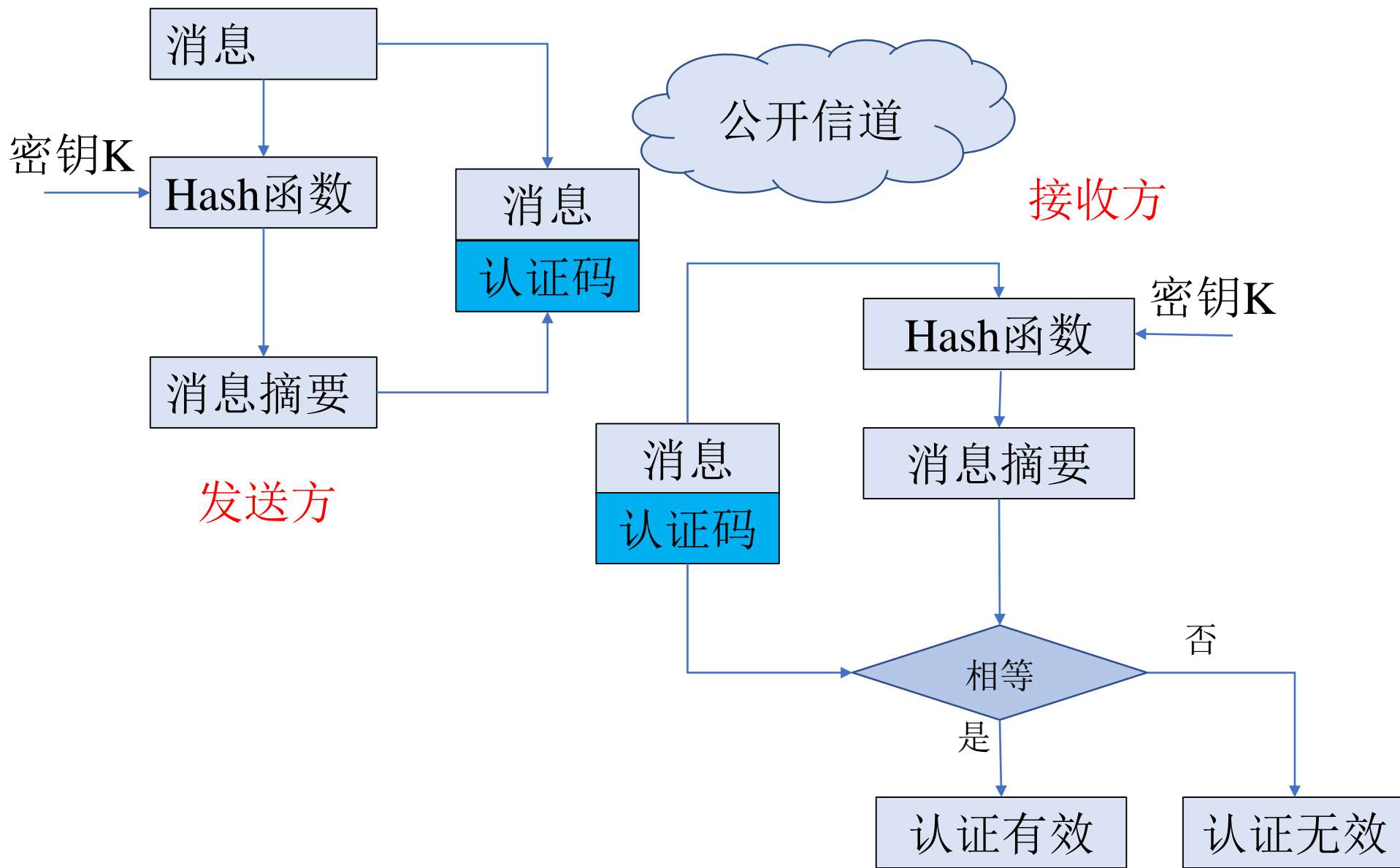


# 消息认证码

- 消息认证码（MAC，Messages Authentication Codes），是与密钥相关的单向散列函数，也称为消息鉴别码或是消息校验和。
- MAC与单向散列函数一样，但是还包括一个密钥。不同的密钥会产生不同的散列函数，这样就能在验证发送者的消息没有经过篡改的同时，验证是由哪一个发送者发送的。



# 消息认证码的实现过程





# 认证小结

- 口令不足以保护重要资源，但具有成本低、易实现等特点。
- 认证令牌，特别是时间令牌，是基于口令的强认证方式。
- X.509（数字证书）的认证方式是安全的，但依赖于PKI平台。
- 生物特征认证是复杂的，成熟的，有较好的应用前景。
- 消息认证码MAC是安全和高效率的。



# 作业



1. 口令认证的基本模式；该模式的不足之处；如何弥补这些不足。