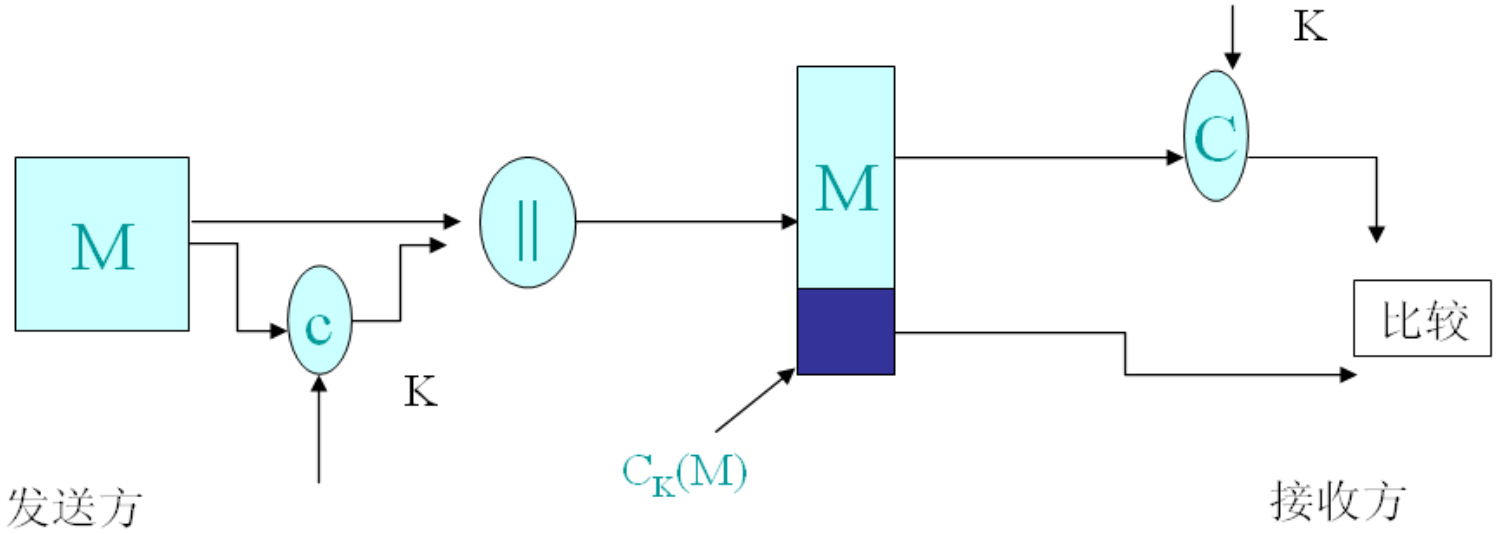
认证技术

问题 3 ：

如何进行消息认证后的防抵赖？

消息认证码的基本用途 1

1． 只提供消息认证，不提供保密性

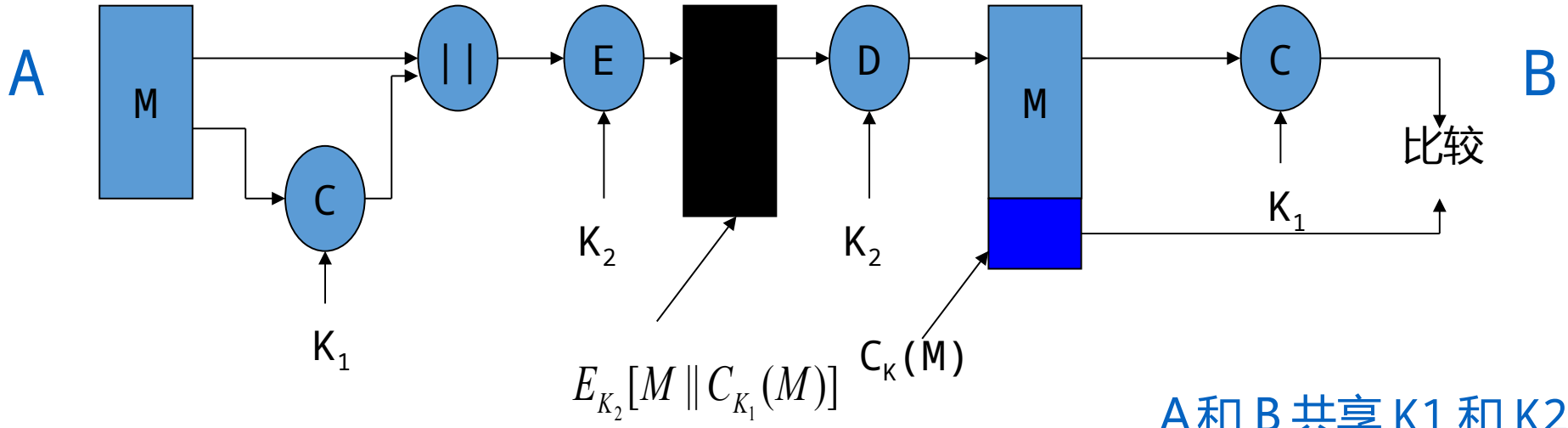


- 消息认证码 MAC ： $MAC = C_k(M)$
  - 确认消息未被更改过
  - 确信消息来自于与他共享密钥的发送者

- A 和 B 共享密钥 K
- A 计算 $MAC=C_k(M)$，
- M和 MAC 一起发送到 B
- B 对收到的 M，计算 MAC ，比较两个 MAC 是否相同。

消息认证码的基本用途 2

- 2． 提供消息认证和保密性：与明文有关的认证



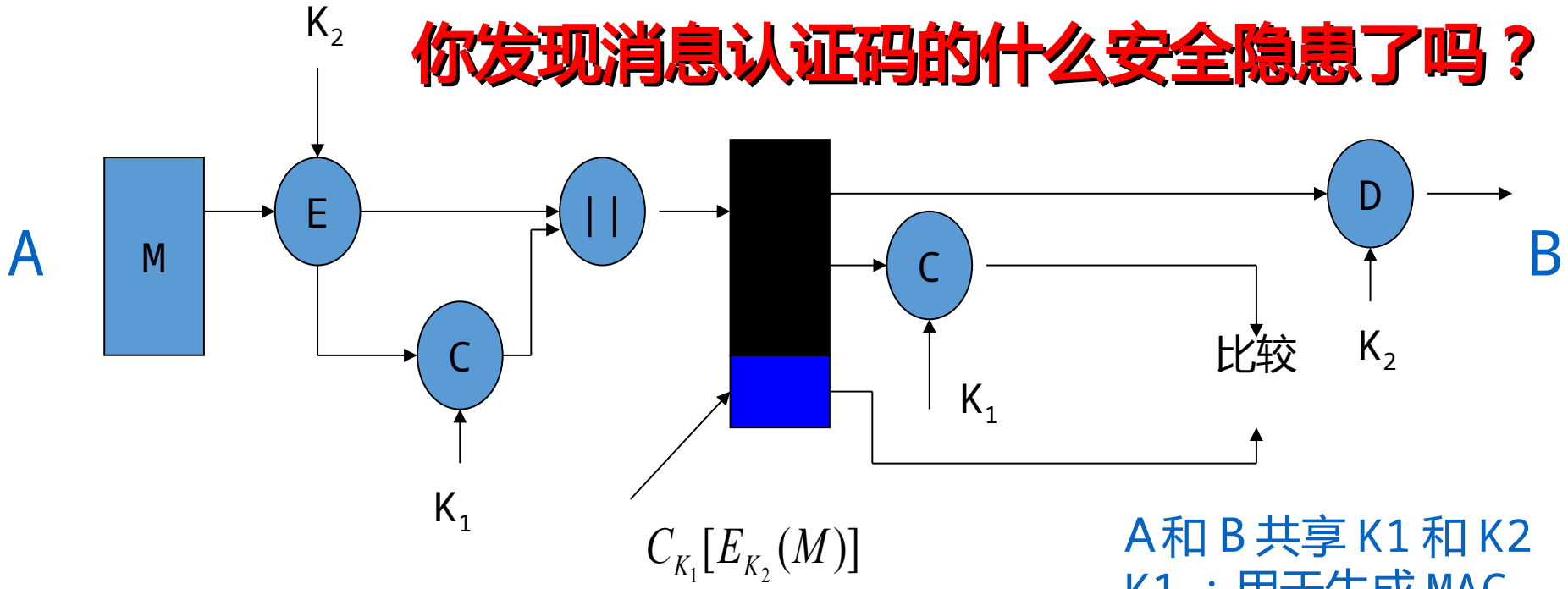
A和 B 共享 K1 和 K2
K1 ：用于生成 MAC
K2 ：用于加密

- 发送方发送 $E_{k2}[M||C_{k1}(M)]$。
- 该种处理方式除具备（1）的功能外，还具有保密性。

消息认证码的基本用途 3

- 3．提供消息认证和保密性：与密文有关的认证

你发现消息认证码的什么安全隐患了吗？



A和 B 共享 K1 和 K2
K1 ：用于生成 MAC
K2 ：用于加密

- 先对消息进行加密，然后再对密文计算 MAC ，传送 $E_{k2}(M)||C_{k1}(E_{k2}(M))$ 给接收方。
- 接收方先对收到的密文进行认证，认证成功后，再解密。

数字签名

消息认证

- 当收发者之间没有利害冲突时，这对于防止第三者的破坏已经足够了。
  - 收方能够验证消息发送者身份是否被篡改；
  - 收方能够验证所发消息内容是否被篡改。

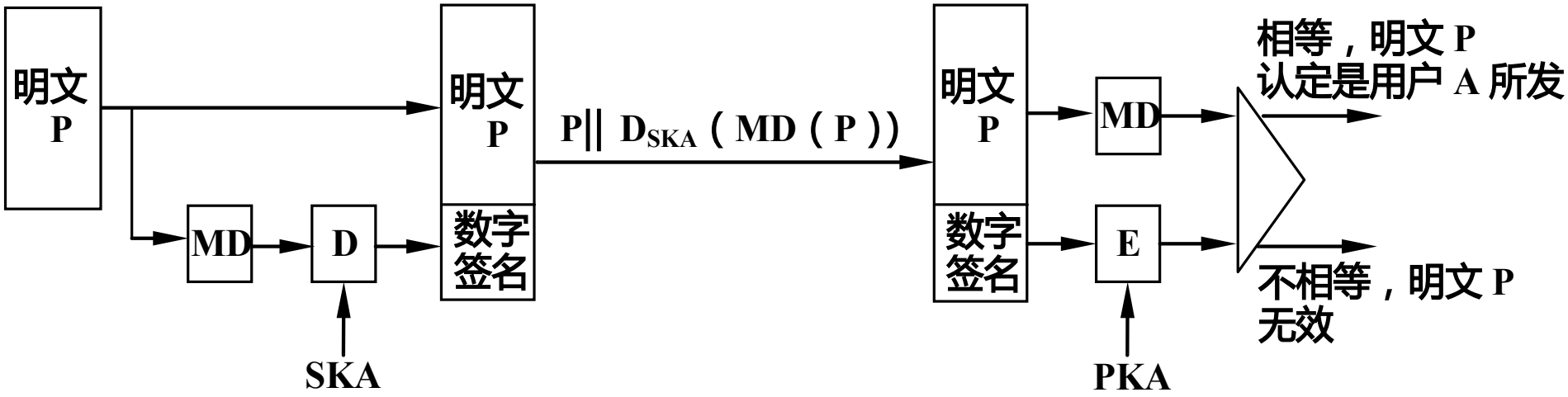
数字签名

- 当收发双方存在利害冲突时，单纯用消息认证技术就无法解决他们之间的纠纷。必须使用数字签名技术。
  - 数字签名能确定消息来源的真实性
  - 数字签名能保证实体身份的真实性
  - 数字签名是不可否认的。

数字签名

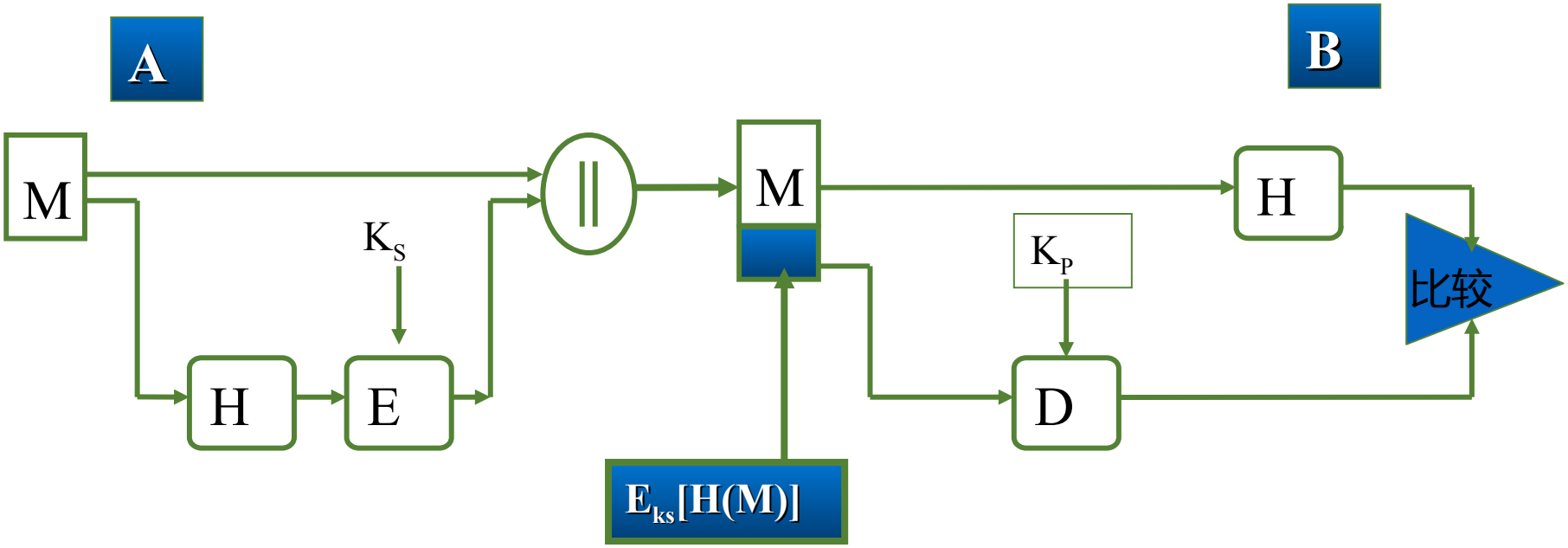
- 数字签名离不开公钥密码学，在公钥密码学中，密钥由*公开密钥*和*私有密钥*组成。数字签名包含两个过程：
  - 签名过程：请问使用什么密钥进行签名？
  - 验证过程：请问使用什么密钥进行验证？

数字签名



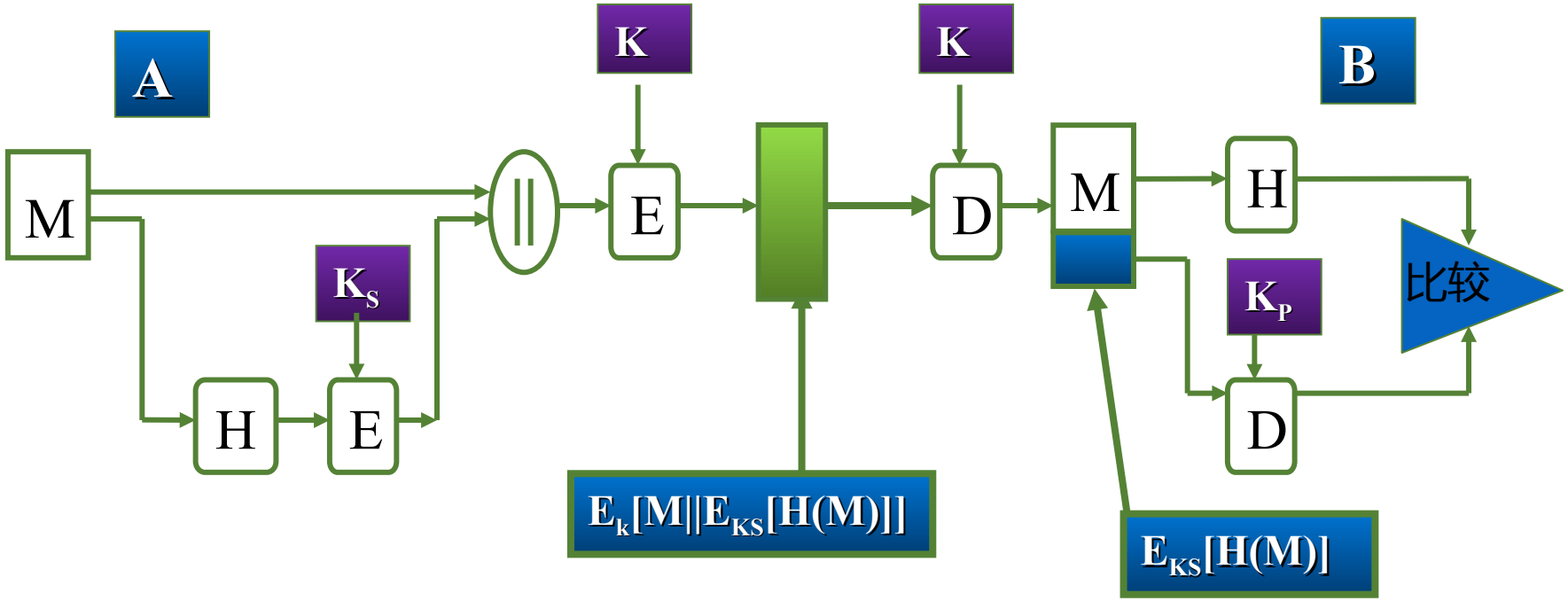
- 规则一： E_{PKA}（D_{SKA}（P））=P，通过公钥 PKA 加密还原的一定是通过私钥 SKA 解密运算的结果；
- 规则二：无法根据报文摘要 h，求出报文 X，且使得 MD（X）＝h；

数字签名



加密/签名结合应用方案

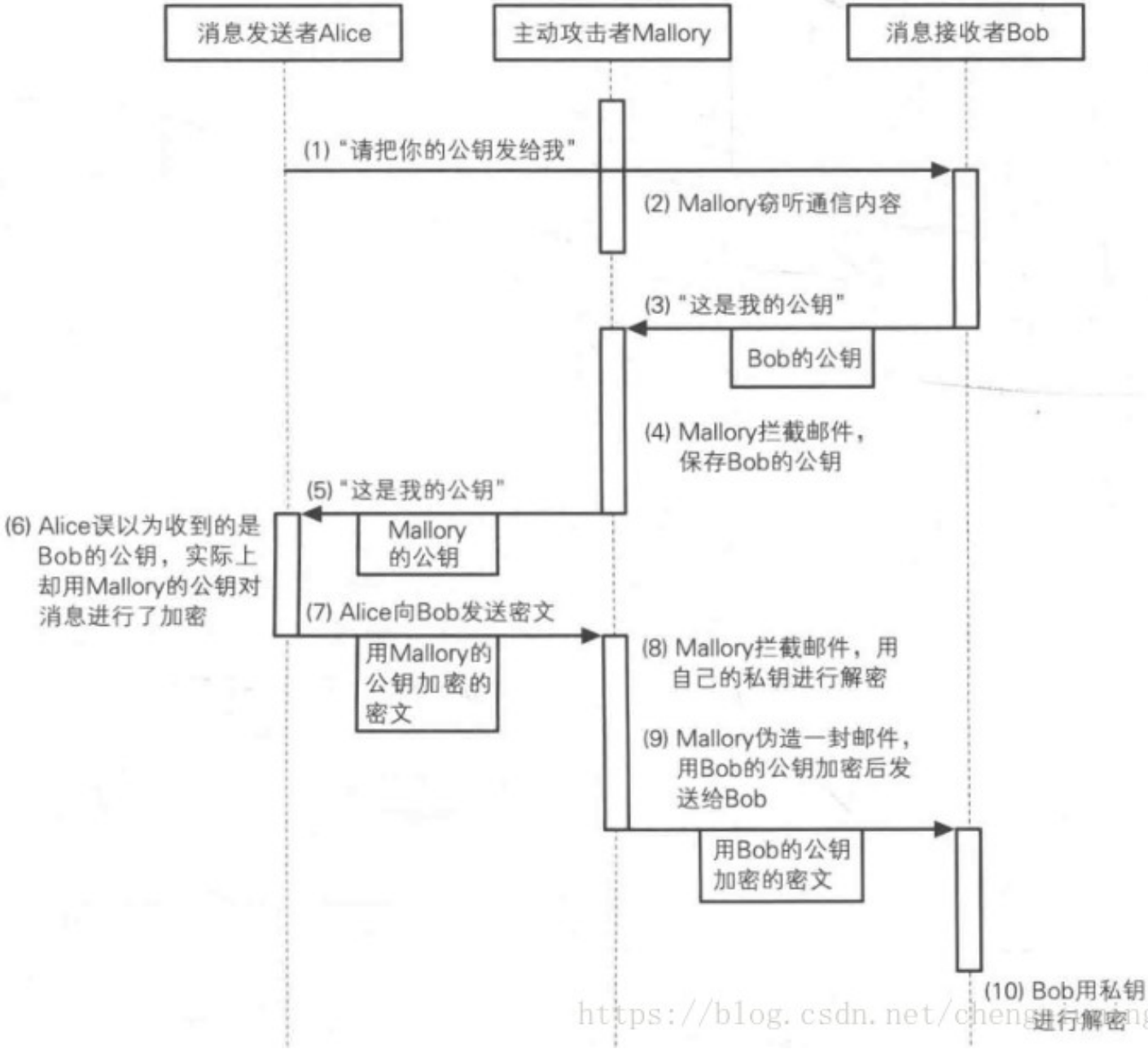
既提供保密性，又提供数字签名



思考：

你发现“数字
存在什么安全

中间人攻击



问题 4 ：

用户如何宣告自己的公钥
确保不遭受中间人攻击？

PKI

- 怎样分发和获取用户的公钥？
- 如何建立和维护用户与其公钥的对应关系？
- 获得公钥后如何鉴别该公钥的有效性？
- 通信双方如果发生争议如何仲裁？

PKI

- **公钥基础设施 PKI**（ Public Key Infrastructure ）的本质是实现大规模网络中的**公钥分发**问题，建立大规模网络中的**信任基础**。

- PKI 在实际应用中是一套**软硬件系统**和安全策略的集合，它提供了一整套**安全机制，**使用户在不知道对方身份或分布地点的情况下，以**数字证书**为基础，通过一系列的信任关系进行网络通信和网络交易。

PKI

- PKI 的组成

（ 1 ）数字证书（ 也称作

（ 2 ）注册授权中心 RA

（ 3 ）认证授权中心 CA

（ 4 ）数字证书库是存储

PKI

- **基于 PKI 的身份认证机制**

出示身份标识信息，如用户 A 的公钥 K_A、电话号码等

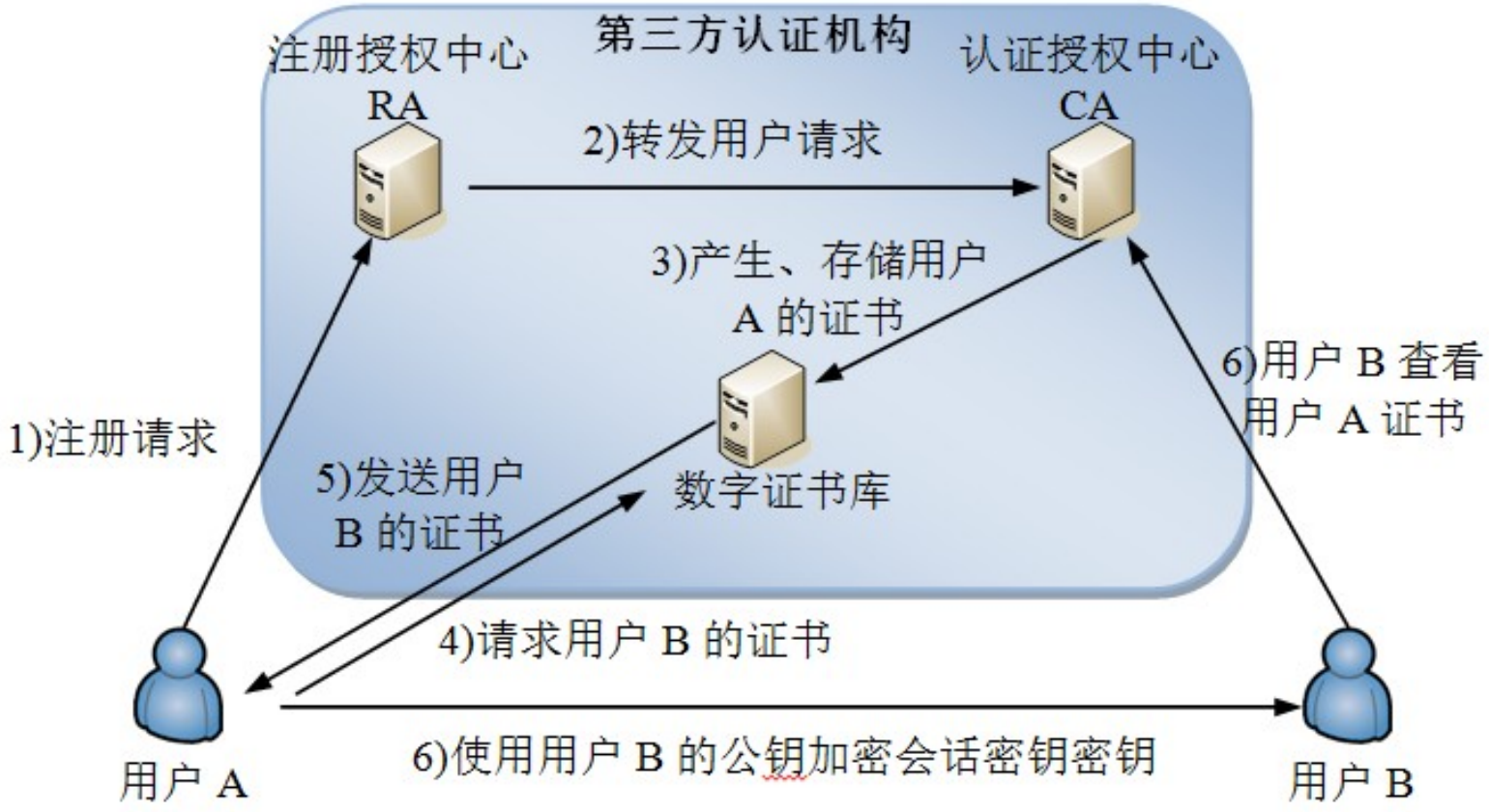
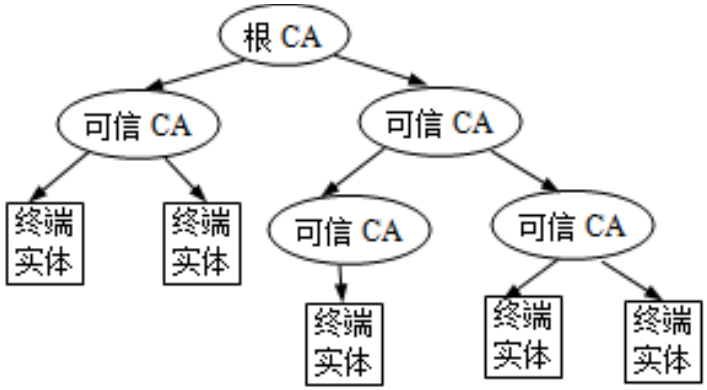
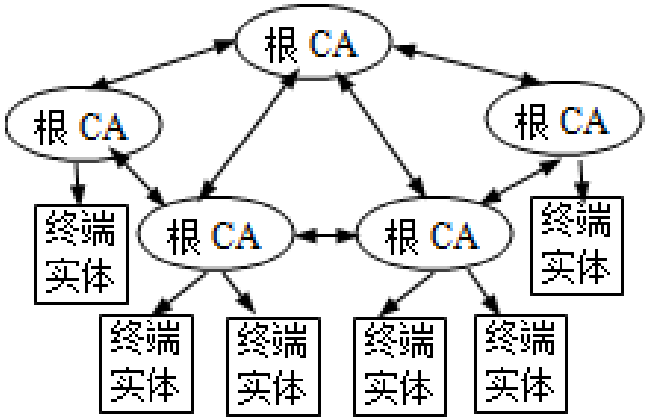


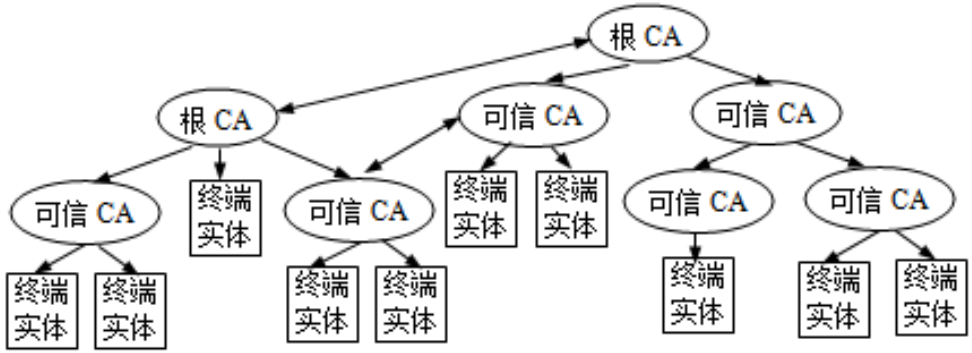
图 4-21　PKI 的基本工作流程图

PKI

- 基于 PKI 的身份认证机制







问题 5 ：

用户在没有公钥证书时，如何证明自己的身份？

身份认证

- 基于所知：口令认证
- 基于所有：身份证件，护照， U盾， IC 卡
- 基于所生：人脸、指纹、视网膜、步态等生物特征

身份认证 - 口令认证再讨论

基于其易用，成本低，易更换等特点，**基于口令的身份认证将长期存在**

口令在应用过程中经历了如下几个阶段：

网络明文传输 + 明文存储

网络明文传输 + 密文存储（加密或者 hash ）

网络密文传输 + 密文存储（加密或者 hash ）

网络密文传输 + 密文存储（加密或者 hash ）**+ 口令保护（诱饵口令检测，基于门限密码实现多方分片存储、基于机器相关函数设计 hash 结果）**

wangding@nankai.edu.cn
http://wangdingg.weebly.com/
August 2021 • Tianjin, China

身份认证 - 基于所有

- 基于所有的身份认证，离不开可信第三方。
- 与 PKI 的整个设计思路类似
- 应用广泛，但存在使用不便利，成本高的特点

身份认证 - 基于所生

- 基于所生的身份认证，方便使用，不能更换。
- 认证使用的信息属于个人敏感数据，被恶意利用的风险大。
- 基于所生的身份认证，普遍存在误判，漏判的区间，依赖算法及参数配置。

课堂讨论：设置最强个人密码（口令）

- CSDN 杯选出的 我最喜欢的密码”

你自己的安全密码？

- **季军**：

FLZX3000cY4yhx9day（飞流直下三千尺，疑似银河下九天）
hanshansi.location()!∈[gusucity]（姑苏城外寒山寺）
hold?fish:palm （鱼和熊掌不可兼得）

亚军：

Tree_0f0=sprintf("2_Bird_ff0/a")（两个黄鹂鸣翠柳 ）；
csbt34.ydhl12s （池上碧苔三四点，叶底黄鹂一两声）；
for_$n(@RenSheng)_$n+="die"（人生自古谁无死）

CSDN 杯我最喜欢的密码大决选**总冠军**：
ppnn13%dkstFeb.1st 。（娉娉裊裊十三余，豆蔻梢头二月初。）

课堂讨论：展望未来的个人密码管理

- 未来元宇宙中，用户的密钥管理的形式应该是什么样？

- 元宇宙从 2021 年快速进入人们的视野，数字人可谓元宇宙中非常活跃的重要实体。虽然现阶段数字人更多的是一些游戏的化身，但是随着技术的发展，数字人和物理社会的自然人是必将一一绑定的，自然人通过数字人在元宇宙中完成学习、工作和娱乐。
- 换句话说，用户，自然人，将在海量的信息系统中完成学习、工作和娱乐等，将会面临海量的身份认证，那么海量的认证所需要的秘密因子——密钥，该怎么完成生成、存储和使用、销毁呢？？

小结

问题 1 ：如何进行完整性检测

问题 2 ：如何进行完整性检测的同时防消息伪造？

问题 3 ：如何进行消息认证后的防抵赖？

问题 4 ： 用户如何宣告自己的公钥确保不遭受中间人攻击？

问题 5 ： 用户在没有公钥证书时，如何证明自己的身份？