福昕PDF编辑器 个人版

• 永久 • 轻巧 • 自由

立即下载

购买会员

永久使用

无限制使用次数

极速轻巧

超低资源占用，告别卡顿慢

自由编辑

享受Word一样的编辑自由

扫一扫，关注公众号

http://edit.foxitreader.cn

网络安全基础

学习内容

- 对称密钥加密
- 不对称密钥加密

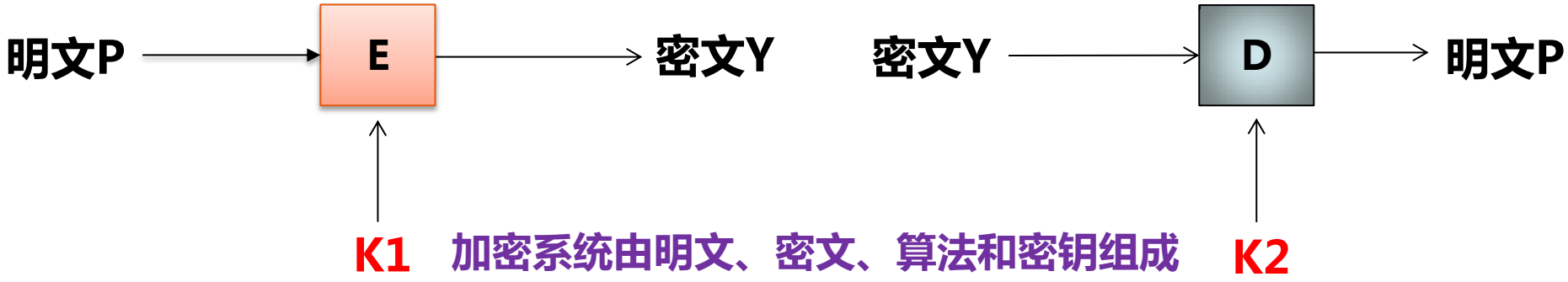
数据加密

- **数据加密**是指将一个信息（或称明文）经过**密钥**及**加密函数**转换，变成无意义的**密文**，而接收方则将此密文经过**解密函数**、**密钥**还原成明文的过程。
- 加密是一种数据转换，解密是加密的逆转换，数据加密是网络安全技术的基石

加密过程为：$Y=E_{K1}(P)$

解密过程为：$P=D_{K2}(Y)=D_{K2}(E_{K1}(P))$

数据加密主要为了防止信息泄露



- 对称密钥加密：加密密钥K1**等于**解密密钥K2
- 不对称密钥加密：加密密钥K1**不等于**解密密钥K2

数据加密

一、对称密钥加密

加密和解密算法都是公开的，重点保证密钥安全性：

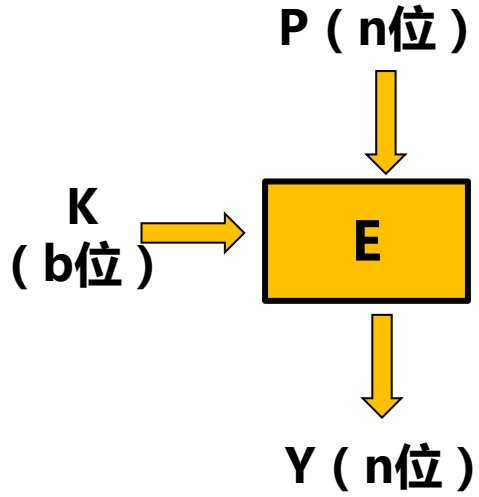
- **分组密码：**黑客无法在知道加密解密算法的情况下，通过有限的密文Y及对应的明文P推导出密钥K，算法复杂
- **序列密码：**每一个密钥只进行一次加密运算，而且每一个密钥都是从一个足够大的密钥集中随机产生，密钥之间没有任何相关性

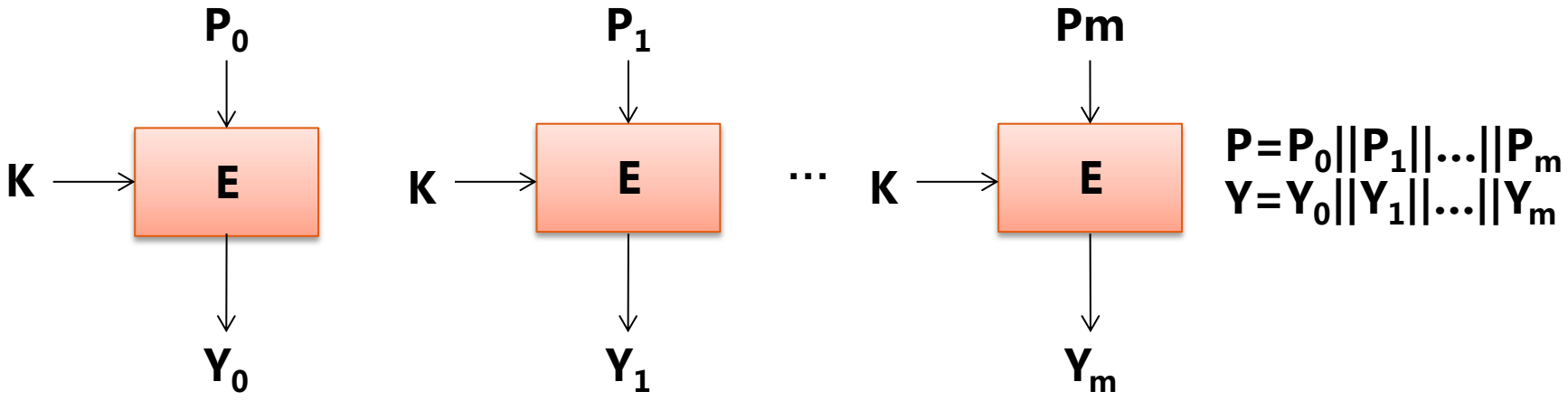
数据加密：对称密钥加密

（一）分组密码

1、分组密码体制的本质含义

- 将明文分割成固定长度的数据段，然后单独对每一段数据进行加密运算，产生和数据段长度相同的密文，密文序列和明文分组产生的数据段序列一一对应。
- 解密运算过程就是将密文还原为对应数据段的过程。





数据加密：对称密钥加密

（一）分组密码

2、常见的分组密码加密算法

- 数据加密标准（Data Encryption Standard ，DES）
  - 密钥长度和数据段长度均为64位
  - 加密运算前，将数据分为64位长度的数据段，然后对每一段数据段进行加密运算
  - 产生64位长度的密文
- 高级加密标准（Advanced Encryption Standard ，AES）
  - 密钥长度可以是128位、192位或者256位，数据段长度固定为128位
  - 加密运算前，将数据分为128位长度的数据段，然后对每一段数据段进行加密运算
  - 产生128位长度的密文

数据加密：对称密钥加密

（一）分组密码

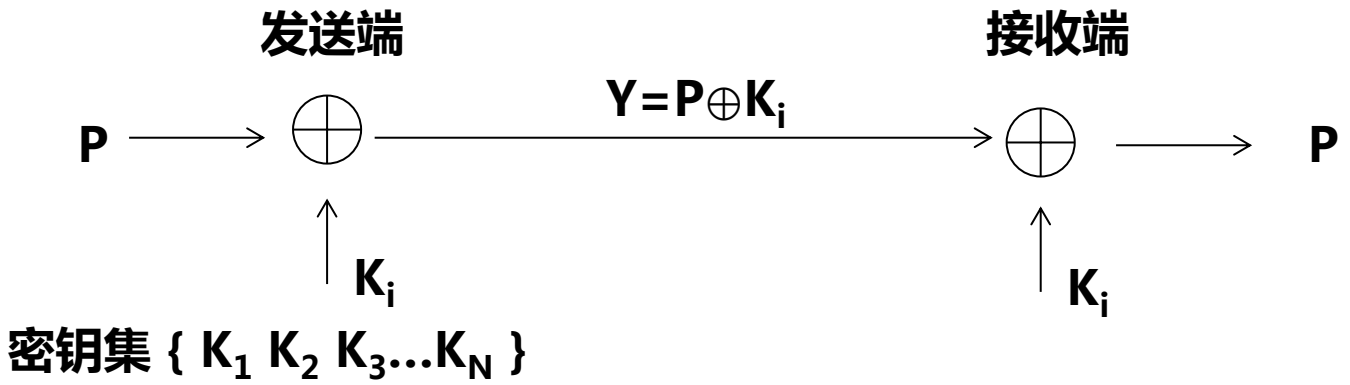
2、常见的分组密码加密算法的安全性

- **数据段长度**：增加数据段的长度，有利于提高加密算法的安全性（不容易通过明文、密文对解析出密钥），但增加运算复杂性
- **密钥长度**：增加密钥的长度，有利于提高加密算法的安全性，但增加运算复杂性。

数据加密：对称密钥加密

（二）序列密码

序列密码（也称流密码）体制就是一次一密钥的加密运算过程。

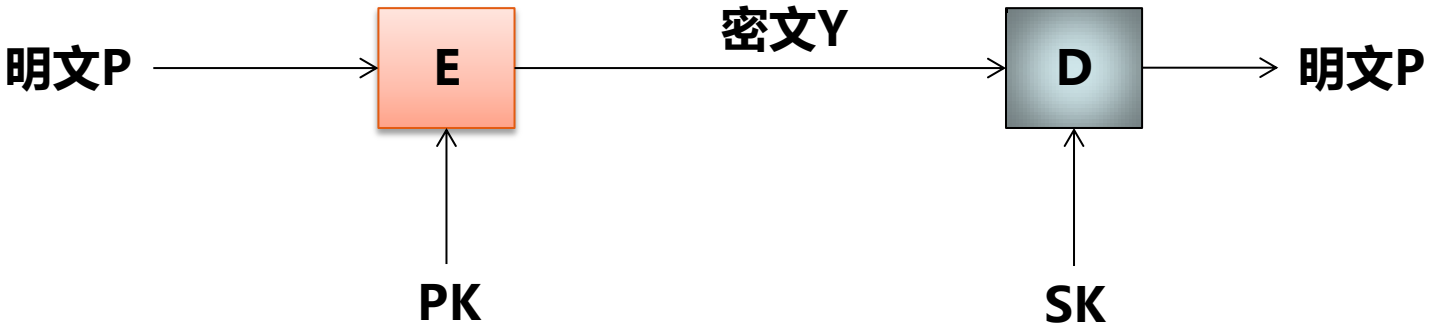


流密码体制的限制：

- 密钥集总是有限的
- 密钥集中的密钥是用算法产生的，密钥之间无法做到没有任何相关性
- 发送端和接收端每次数据传输过程都必须同步密钥

数据加密

二、不对称密钥加密算法



- 公开密钥加密算法是一种不对称密钥加密算法
- 公开密钥加密算法使用不同的加密密钥和解密密钥

数据加密

二、不对称密钥加密

公开密钥加密

公开密钥加密算法的原则：

- 容易成对生成密钥PK和SK，且PK和SK一一对应
- 加密和解密算法是公开的，而且可以对调

$$D_{SK}(E_{PK}(P)) = E_{PK}(D_{SK}(P)) = P$$

- 加密和解密过程容易实现
- 从计算可行性讲，无法根据PK推导出SK
- 从计算可行性讲，如果$Y=E_{PK}(P)$，无法根据PK和密文Y推导出明文P

数据加密

二、不对称密钥加密

公开密钥加密

- RSA（Rivest-Shamir-Adelman）是目前最常用的公开密钥加密算法
- RSA私钥的安全性取决于密钥长度n，当n为1024位二进制数时，根据目前的计算能力，RSA私钥的安全性是可以保证的
- n越大，加密和解密运算的计算复杂度越高

小结

- 信息安全的基础是加密
- 保密性是信息安全的核心目标
- 加密算法分为对称密钥加密算法和不对称密钥加密算法
- 对称密钥加密算法的计算复杂度远小于不对称密钥加密算法的计算复杂度
- 通常用对称密钥加密算法加密数据，不对称密钥加密算法加密对称密钥加密算法所使用的密钥

学习内容

- 报文摘要
- 数字签名
- 身份鉴别

报文摘要

报文摘要（MD）技术是一种检查发送的报文是否被篡改的方法

（1）给定某个任意报文

（2）通过一种特定的算法对报文进行计算，产生有限位数信息，即

报文摘要，报文摘要就像报文的指纹一样，具有：

- 确认性
- 唯一性

报文摘要

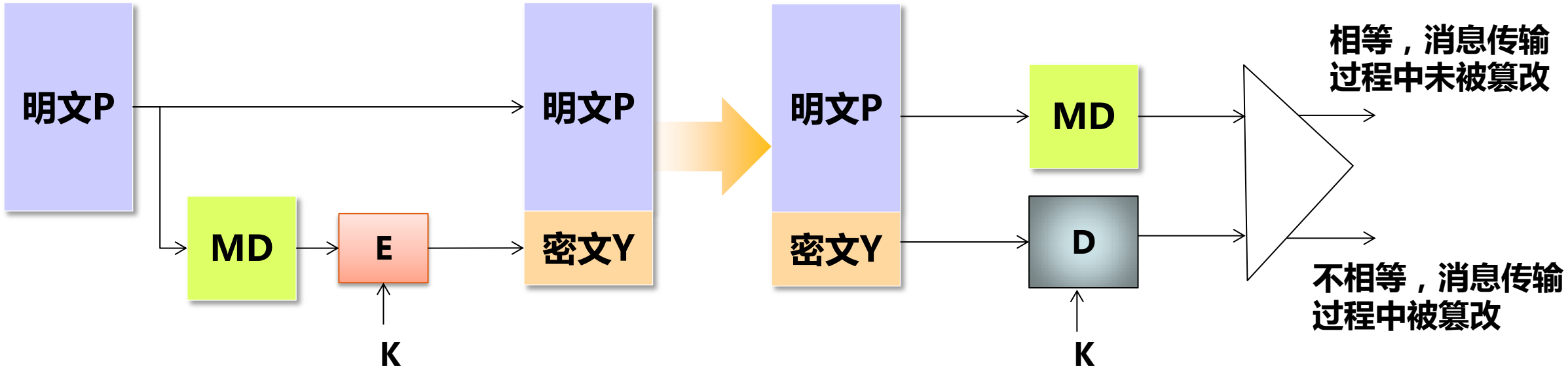
假定MD为报文摘要算法，MD（X）是算法对报文X作用后产生的标识信息（即报文摘要），MD必须满足如下要求：

- 能够作用于任意长度的报文
- 产生有限位数的标识信息
- 易于实现
- 具有单向性，即只能根据报文X求出MD（X），从计算可行性讲，无法根据标识信息h，得出报文X，且使得MD（X）=h
- 具有抗碰撞性，即从计算可行性讲，对于任何报文X，无法找出另一个报文Y，X≠Y，但MD（X）=MD（Y）
- 即使只改变报文X中一位二进制位，也使得重新计算后的MD（X）变化很大

报文摘要

2．报文摘要的主要用途

（1）消息完整性检测



（a）发送端操作过程

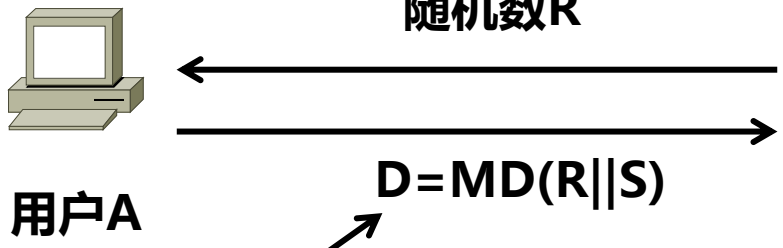
（b）接收端操作过程

报文摘要

2．报文摘要的主要用途

（1）消息完整性检测

（2）验证秘密信息：**身份鉴别**



S：用户A需要验证的秘密信息

用户B拥有用户A与S的对应关系

用户名	秘密信息
用户A	S

用户A把R与S串接后求报文摘要

用户B把R与S串接后求报文摘要D’ =MD(R||S)

D’ =D？

是：验证通过

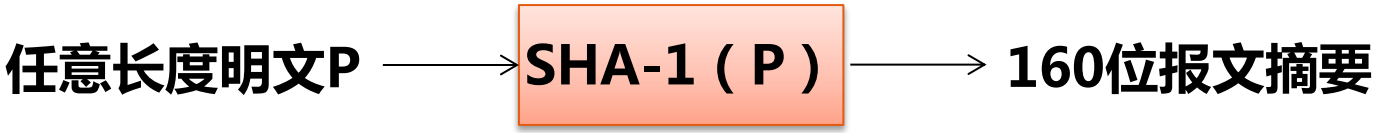
不是：验证不通过

报文摘要

3．几种常用的报文摘要算法

（1）MD5：报文摘要第5版（Message Digest ,Version 5，MD5）

（2）SHA-1：安全散列算法第1版（Secure Hash Algorithm 1， SHA-1）

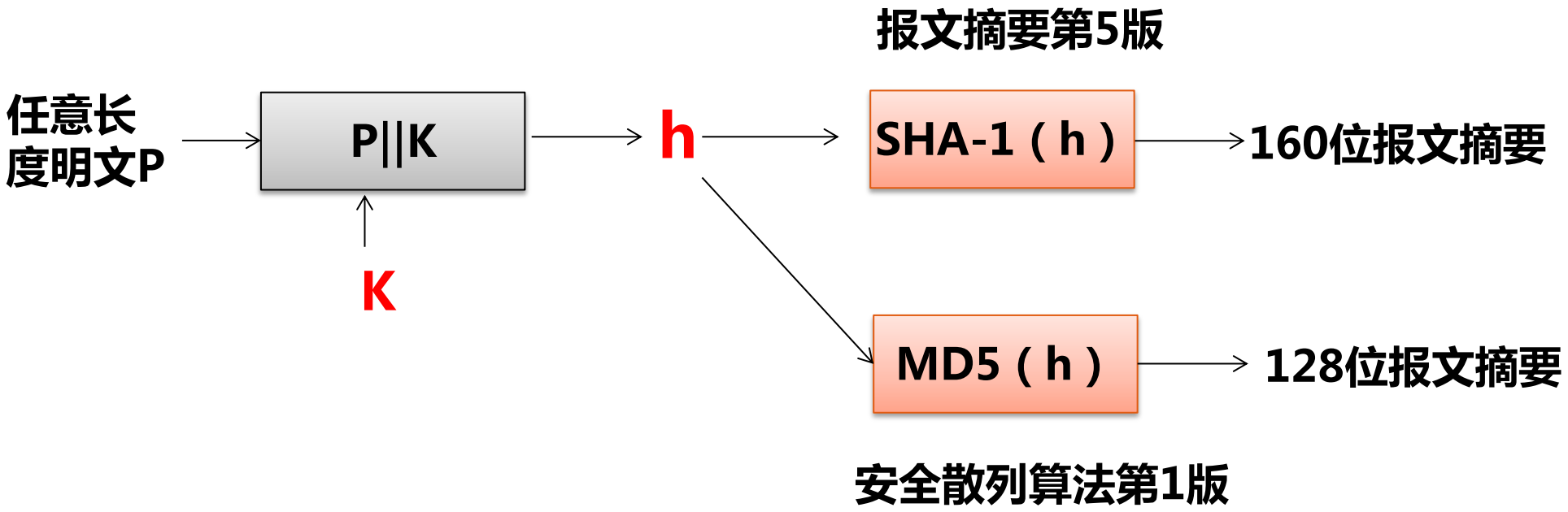


报文摘要

3．几种常用的报文摘要算法

（3）HMAC：散列消息鉴别码

（Hashed Message Authentication Codes ，HMAC）



用HMAC-MD_K（P）表示报文P基于密钥K和报文摘要算法MD生成的报文摘要

报文摘要

4．报文摘要算法的安全性因素

报文摘要的位数越大:

- 计算复杂性越高
- 单向性和抗碰撞性越好

数字签名

1．数字签名特征

数字签名就是只有信息发送者才能产生的、别人无法伪造的一段数字串，这段数字串同时也是对信息发送者发送信息真实性的一个有效证明，它具有如下特征：

- 接收者能够**核实**发送者对报文的数字签名
- 发送者事后**无法否认**对报文的数字签名接
- 接收者**无法伪造**发送者对报文的数字签名

数字签名

1．数字签名特征

数字签名必须保证唯一性、关联性和可证明性

- 唯一性保证只有特定发送者能生成数字签名
- 关联性保证是对特定报文的数字签名
- 可证明性表明该数字签名的唯一性和与特定报文的关联性可以得到证明

数字签名

2．基于RSA数字签名原理

（1）RSA公开密钥加密算法特点

①存在公钥和私钥对PK和SK，PK与SK一一对应

②SK是秘密的，只有拥有者知道，PK是公开的

③无法通过PK推导出SK

④$E_{PK}（D_{SK}（P））=P$

因此，$D_{SK}（MD（P））$可以作为SK拥有者对报文P的数字签名。

数字签名

2．基于RSA数字签名原理

（2）D_{SK}（MD（P））能够作为数字签名的依据

①SK是唯一的，只有SK拥有者才能实现D_{SK}（MD（P）），保证数字签名的**唯一性**；

②根据报文摘要算法特性，其他用户无法做到：生成某个报文P′，P≠P′，但MD（P）= MD（P′），MD（P）只能是针对报文P的报文摘要，保证数字签名和报文P之间的**关联性**；

③因公钥PK和私钥SK一一对应，若公钥PK和SK拥有者之间的绑定关系得到权威机构证明，一旦证明用公钥PK对数字签名进行还原的结果（E_{PK}（数字签名））等于报文P的报文摘要（MD（P）），就可证明数字签名是D_{SK}（MD（P）），保证数字签名的**可证明性**。

颁发

私钥：SK

证书

权威机构CA

SKA：CA的私钥

PKA：CA的公钥

申请证书：

出示各种证件、

证明材料，签署协议

身份+PK

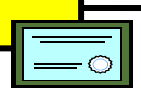
D_{SKA}(MD(身份+公钥))

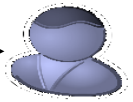
CA对用户身份签名

签名：

P

D_{SK}(MD(P))



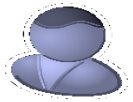


验证签名

1、用CA的公钥PKA验证用户证书

2、用证书的公钥PK验证用户的签名

仲裁：

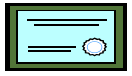


向法庭出示：

P

D_{SK}(MD(P))

的证书



向法庭出示：

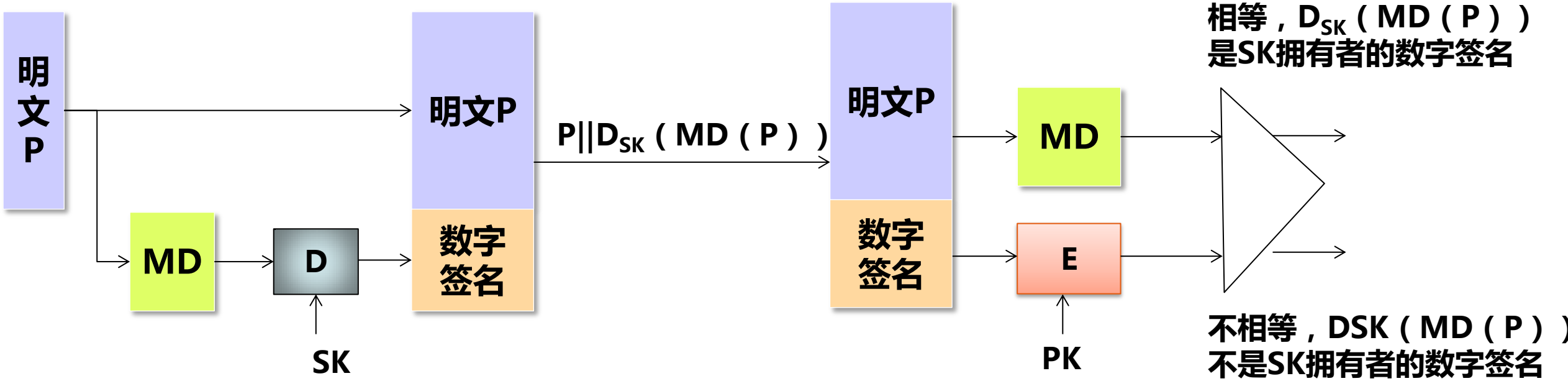
的各种材料及签名

如何仲裁？

数字签名

2．基于RSA数字签名原理

（3）数字签名实现过程



身份鉴别

- 身份鉴别过程：网络中证明自己身份的过程，或是确定通信的另一方的身份的过程
- 用于证明自己身份的一方称为用户，用于确认通信的另一方的身份的一方称为鉴别者
- 用户与鉴别者共享密钥，且该密钥只有用户和鉴别者拥有，因此，一方只要证明自己拥有该密钥，即可证明自己身份

身份鉴别

1．单向鉴别过程

- 单向鉴别过程中只需要用户向鉴别者证明自己身份，无需确认鉴别者身份
- 用户A向鉴别者证明自己身份的过程就是证明拥有密钥KEYA的过程

身份鉴别

2．双向鉴别过程

- 双向鉴别过程中用户不仅需要向鉴别者证明自己的身份，同时需要确认鉴别者的身份，因此，用户和鉴别者都需证明自己拥有共享密钥
- 用户A和鉴别者都需证明自己拥有共享密钥KEYA

小结

- 完整性是信息安全的核心目标
- 加密和报文摘要实现完整性
- 数字签名实现不可抵赖性