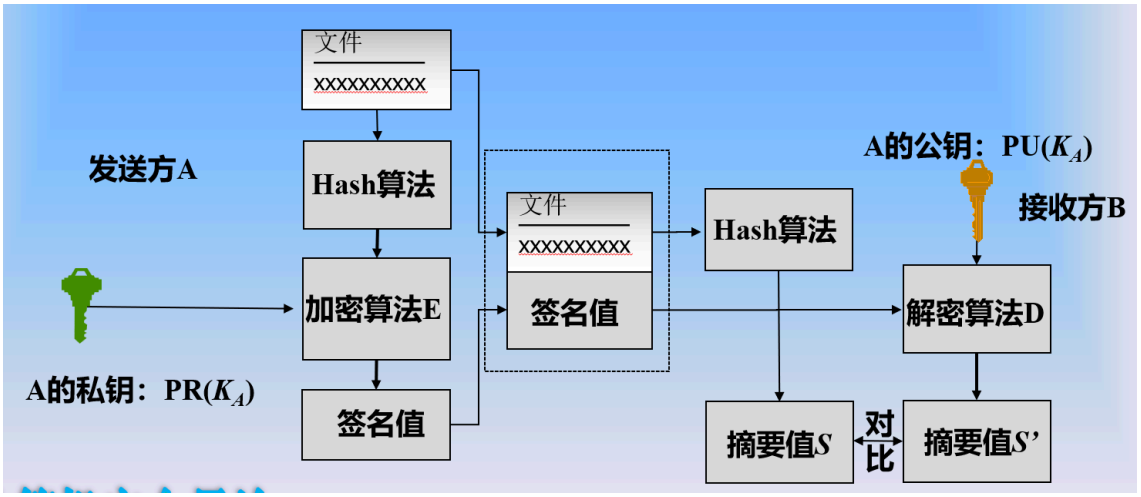
数字签名与散列函数

数字签名

- 作用：
  - 验证作者, 签名日期时间（不可否认性）
  - 验证消息内容 （完整性）
  - 通过第三方认证解决纠纷（公开验证性）
- 原始数字签名方案的缺点
  - 利用公钥密码对整个文件进行加密操作，运行速度受文件大小影响，运行效率低。
  - 加密后的签名文件与原文件一样大小，不利于网络传输，接收方在验证时花费时间过多
- 改进的数字签名方案
  - 发送方A先应用散列函数对文件生成摘要值，再采用A的私钥对摘要值*S*进行签名，将文件与签名值发送给接收方B。
  - 接收方B接收文件与签名值后，对文件进行散列操作生成摘要值*S'*，同时对签名值用A的公钥进行解密生成摘要值*S*，比较*S*与*S'*验证签名。



散列函数

- 定义：一个公开函数，可以将任意长的消息M映射为较短的、固定长度的一个值H(M)。
- 具备的性质：
  - H可适用于任意长度的数据块。
  - H能生成固定长度的输出。
  - 对于任意给定的x，计算H(x)相对容易，并可以用软硬件方式实现。
  - 对于任意给定值h，找到满足**H(x)=h的x**是计算上不可行。满足这一特性的散列函数称为具有单向性，或具有**抗原像攻击性。**
  - 对于任意给定的数据块x，找到**满足H(y)=H(x)的y(不同于x)**是计算上不可行。满足这一特性的散列函数被称为具有**抗第二原像攻击性(抗弱碰撞攻击性)**
  - 找到满足**H(y)=H(x)的任意一对(x,y)**的计算上是不可行的。满足这一特性的散列函数被称为**抗碰撞性（抗强碰撞性）**。
- 安全分析

有两种方法可以攻击一个安全散列函数

- 密码分析法：利用该算法在逻辑上的缺陷。
- 穷举搜索法：安全强度完全依赖于算法生成的散列码长度。攻击一个长度为n的散列码所付出的代价为：

抗原像	2^n
抗第二原像	2^n
抗碰撞	$2^{n/2}$

SHA

3.3 SHA-512介绍

SHA-512以最大长度不超过2^{128}比特的消息作为输入，以1024比特的数据块进行处理，生成512比特的消息摘要输出。