《现代密码学》第九章

密钥管理（二）

本节主要内容

- 密钥管理简介
- 密钥分配
- 密钥协商
- PKI及数字证书简介
- 秘密共享
- 密钥托管

本节主要内容

- 密钥管理简介
- 密钥分配
- 密钥协商
- **PKI及数字证书简介**
  - 公钥的分发问题
  - PKI简介
  - 证书管理
  - PKI其它组件

公钥的分发问题

- 广播式公钥分发：任意通信方将它的公钥发送给另一方或广播给其他通信各方。
- 目录式公钥分发：由可信机构维护一个公开、动态、可访问的公开密钥目录。可以通过可信渠道到可信机构登记并申请增、删、改自己的公钥。其他人可以基于公开渠道访问目录来获取某个登记用户的公钥。
- 公钥管理机构分发：目录管理员负责维护并传递完整密钥给请求用户。

公钥的分发问题

例：Needham-Schroeder密钥协商协议（公钥版本）

① A→KDC: ID_A, ID_B

② KDC→A: $S_{sk_{KDC}}[pk_B, ID_B]$

③ A→B: $E_{pk_B}[N_A, ID_A]$

④ B→KDC: ID_B, ID_A

⑤ KDC→B: $S_{sk_{KDC}}[pk_A, ID_A]$

⑥ B→A: $E_{pk_A}[N_A, N_B]$

⑦ A→B: $E_{pk_B}[N_B]$

⑧ $k_s = h(N_A, N_B)$.

公钥的分发问题

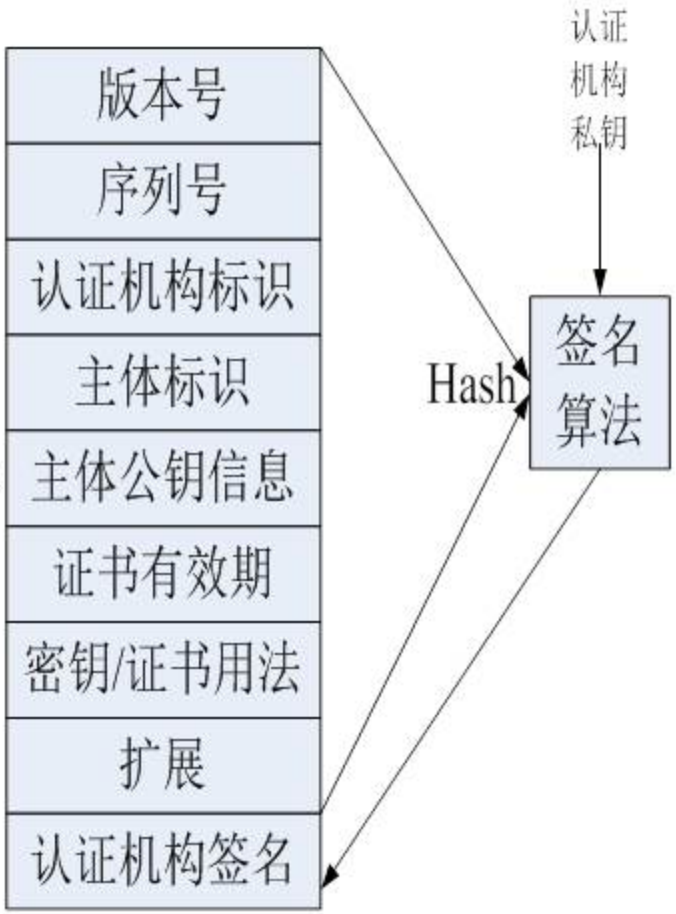
- 数字证书式公钥分发：该方式由Kohnfelder提出，每个参与者向证书中心提交自己的公钥，申请证书。使用公钥时，可向通信对方索取证书或向可信中心索取证书。

- 数字（公钥）证书是一种包含了重要信息的载体，它证明了证书所有人和所持有的公钥的真实性，由一个可信的中介机构进行签名，这可以使获得证书的人只要信任这个可信的中介机构，就可以相信他所获得的证书了。

公钥的分发问题

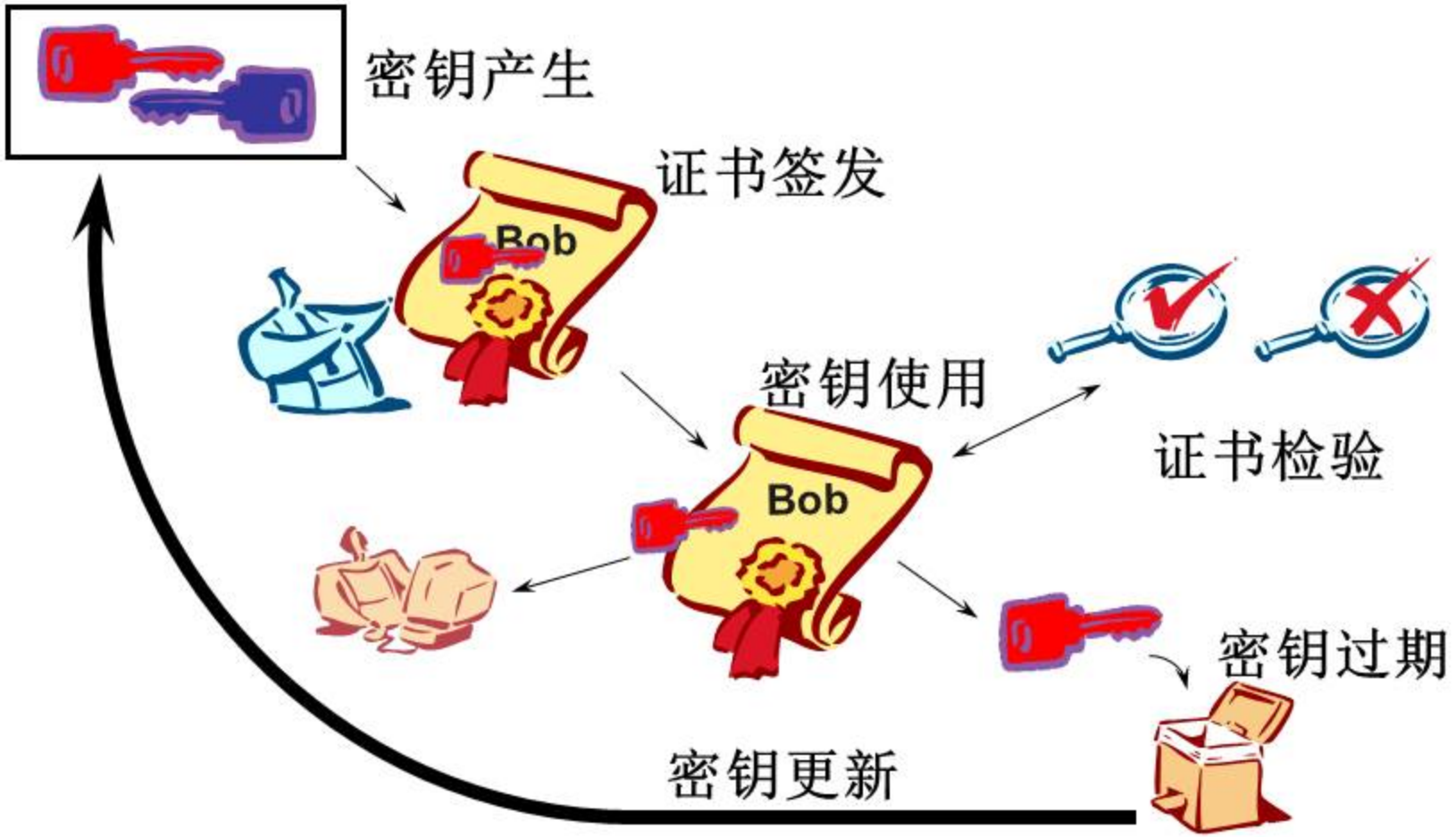
数字证书内容

- 版本号：用来区分X.509的不同版本。
- 序列号：由认证机构给予每一个证书的分配惟一的数字型编号。
- 认证机构标识：颁发该证书的机构惟一的X.500名字。
- 主体标识：证书持有者的名称。
- 主体公钥信息：和该主体私钥相对应的公钥。
- 证书有效期：证书有效时间包括两个日期：证书开始有效期和证书失效期。
- 密钥/证书用法：描述该主体的公/私密钥对的合法用途。
- 扩展：说明该证书的附加信息。
- 认证机构签名：用认证机构的私钥生成的数字签名。



公钥的分发问题

数字证书的生命周期



公钥基础设施简介

公钥基础设施（PKI，Public Key Infrastructure）以公钥技术为基础，将个人、组织、设备的标识信息与各自的公钥捆绑在一起，为用户建立起一个安全、可信的网络运行环境，使陌生用户可以在多种应用环境下方便地使用加密和数字签名技术，在互联网上验证用户的身份，从而保证了互联网上所传输信息的真实性、完整性、机密性和不可否认性。

PKI是生成、管理、存储、分发和吊销基于公钥密码学的公钥证书所需要的硬件、软件、人员、策略和规程的总和。

公钥基础设施简介

（一）注册中心（RA）

- 主体注册证书的个人认证。
- 确定主体所提供信息的有效性。
- 对被请求证书属性确定主体的权利。
- 认证机构代表主体开始注册过程。
- 为识别身份的目的分配名字。
- 在注册初始化和证书获得阶段产生共享秘密。
- 产生公私钥对。
- 在需要撤销时报告报告密钥泄露或终止事件。
- 开始密钥恢复处理。

公钥基础设施简介

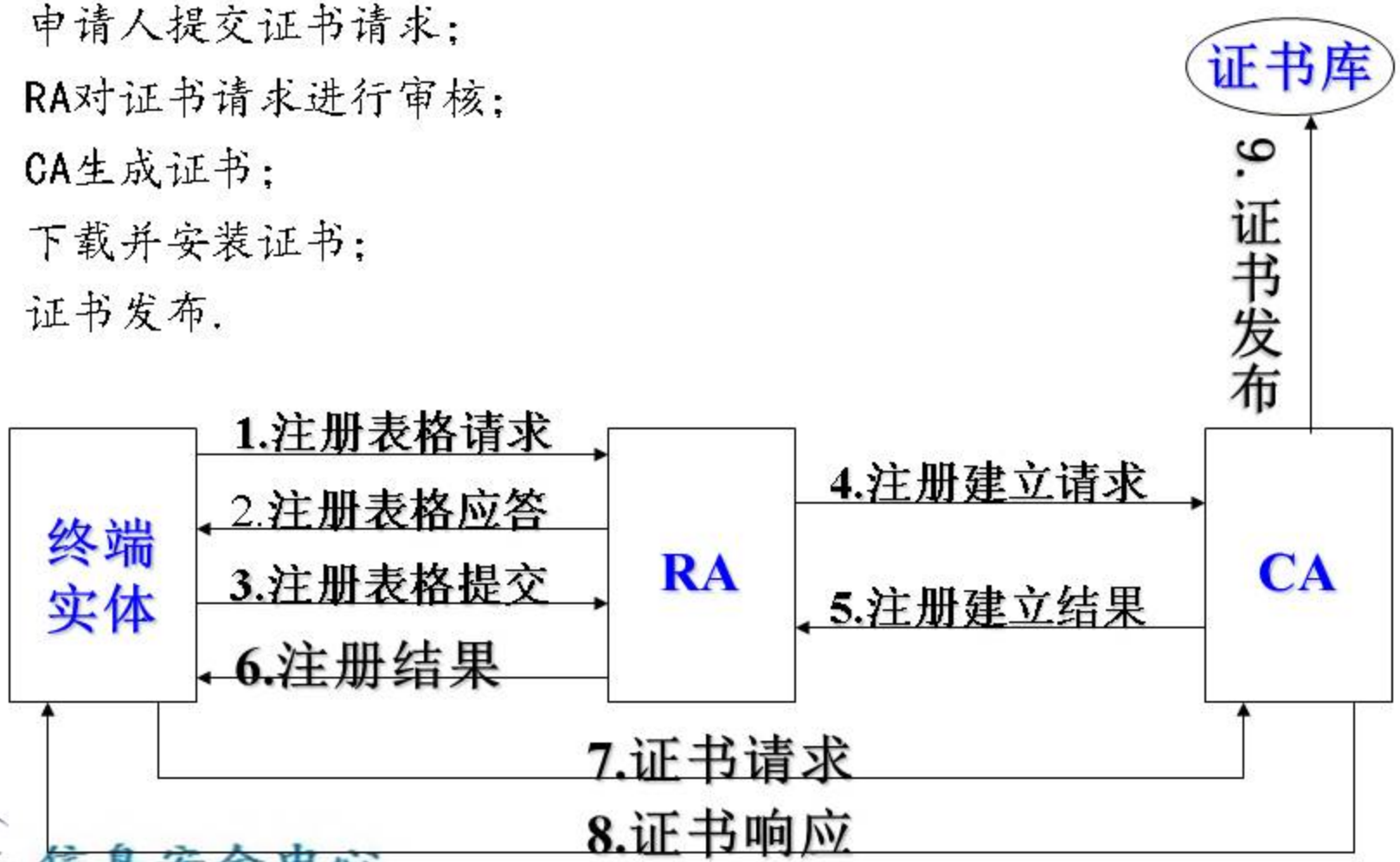
（二）证书授权中心(CA)

- 确定是否接受最终用户数字证书的申请。
- 验证最终用户的公钥是否合法。
- 向申请者颁发、拒绝颁发数字证书。
- 接受、处理最终用户的数字证书更新请求。
- 接受最终用户数字证书的查询、撤销。
- 产生和发布证书注销列表（CRL）。
- 数字证书的归档。
- 密钥归档。
- 历史数据归档。

证书管理

（一）证书注册与发布

- 申请人提交证书请求；
- RA对证书请求进行审核；
- CA生成证书；
- 下载并安装证书；
- 证书发布.



证书管理

（二）证书验证

- 查询该证书是否被CA撤销；
- 检测证书拥有者是否为预期的用户；
- 检查证书的有效期，确保该证书是否有效；
- 检查该证书的预期用途是否符合CA在该证书中指定的所有策略限制；
- 使用CA公钥和算法验证证书签名有效性。

证书管理

（三）证书状态查询

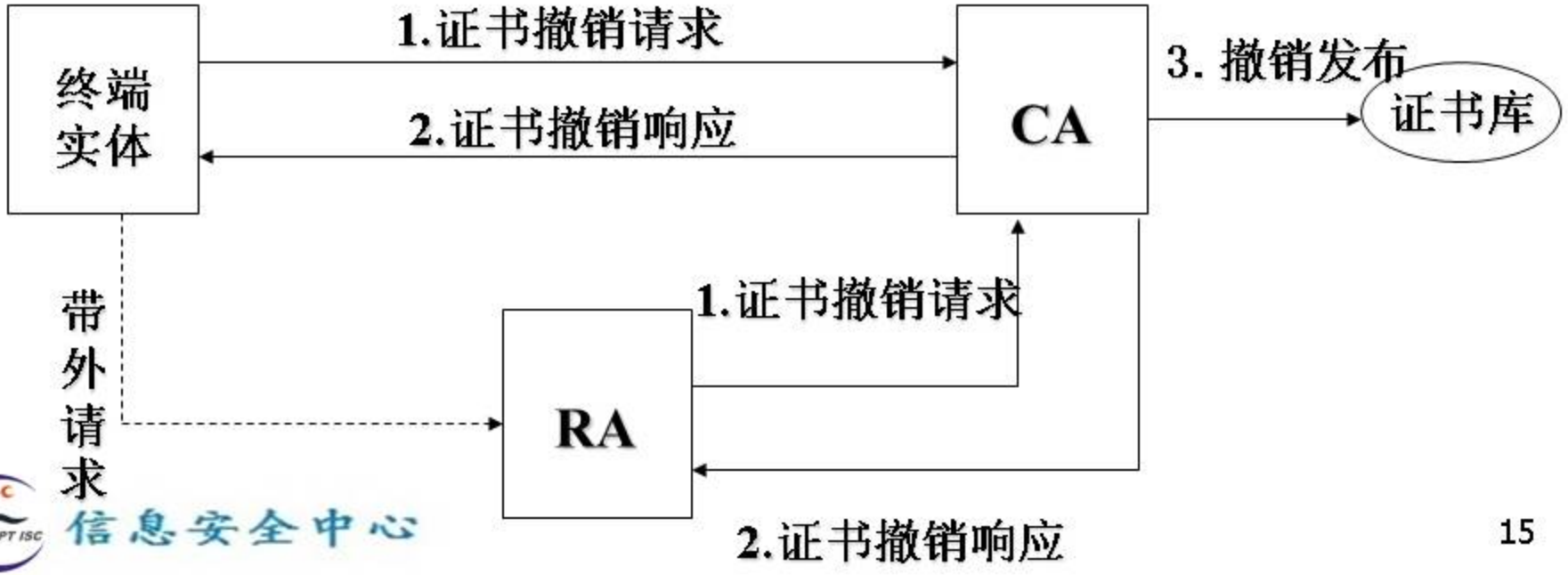
- 在线证书状态协议OCSP（Online Certificate Status Protocol：克服基于CRL的撤销方案的局限性，为证书状态查询提供即时的最新响应。OCSP使用证书序列号、CA名称和公开密钥的散列值作为关键字查询目标的证书。

- 定期下载证书撤销列表（CRL）；

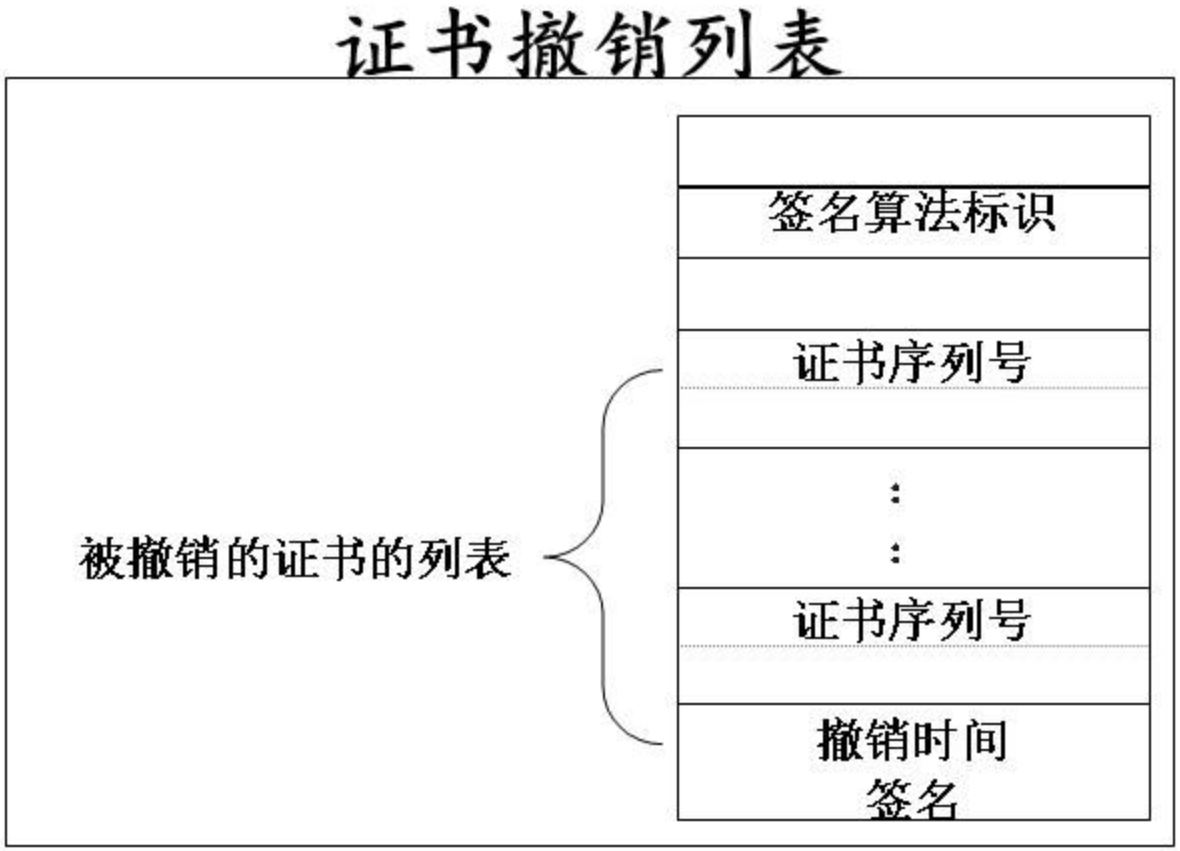
证书管理

（四）证书撤销

- 当条件（雇佣关系结束、证书中信息修改等）要求证书的有效期在证书结束日期之前终止；
- 或者要求用户与私钥分离时（私钥可能以某种方式泄露），证书被撤销。



证书管理



证书管理

（五）证书的更新

- 下列情况需更新最终实体证书

  原证书过期；

  一些属性的改变；

  实体要求发放新证书（如密钥可能泄露）

  CA签名密钥更新

证书管理

（六）证书使用实例

- 简化站-站协议（STS协议）

W.Diffie和P.C.Van Orschot等人于1992年提出DH密钥协商协议的改进协议----站对站协议

（1）协议基于公钥基础设施，存在可信中心CA。设$C(A)$为A的公钥证书，$C(B)$为B的公钥证书

（2）协议利用数字签名技术。

设A的签名算法为Sig_A，签名验证算法为Ver_A；B的签名算法为Sig_B，签名验证算法为Ver_B。

证书管理

设p是一个大素数，$g \in Z_p$是模p的一个本原元，p和g公开。

①用户A随机选取一个大数a，$0 \le a \le p-2$.
计算$K_a = g^a \pmod p$,并将结果传送给用户B.

② B随机选取b, $0 \le b \le p-2$.计算$K_b = g^b \pmod p$，然后计算$K = (K_a)^b \pmod p$和

$$E_B = E_K[Sig_B(g^a \pmod p, g^b \pmod p)]$$

用户B将$(C(B), g^b \pmod p, E_B)$传送给用户A。

证书管理

③ 用户A先验证$C(B)$的有效性。然后计算

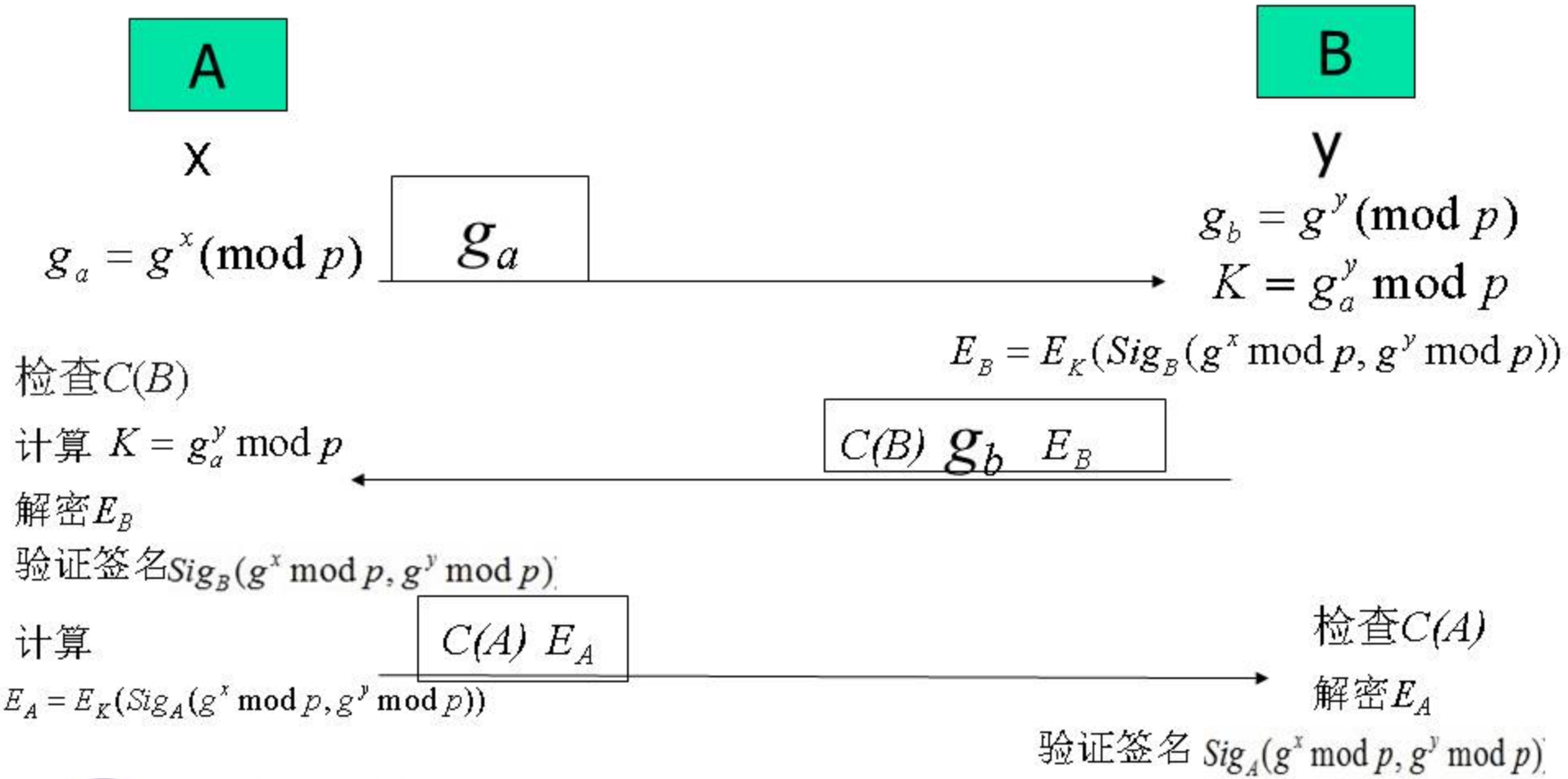
$K=(K_b)^a \pmod p$，解密E_B，再验证B的签名Ver_B. 确认有效后，计算

$$E_A=\mathrm{E}_K[\mathrm{Sig}_\mathrm{A}(g^a \pmod \mathrm{p}, g^b \pmod \mathrm{p}))]$$

把自己的公钥证书$C(A)$以及E_A发给用户B。

(4) 用户B解密后，验证$C(A)$的有效性，再解密验证A的签名Ver_A.

证书管理

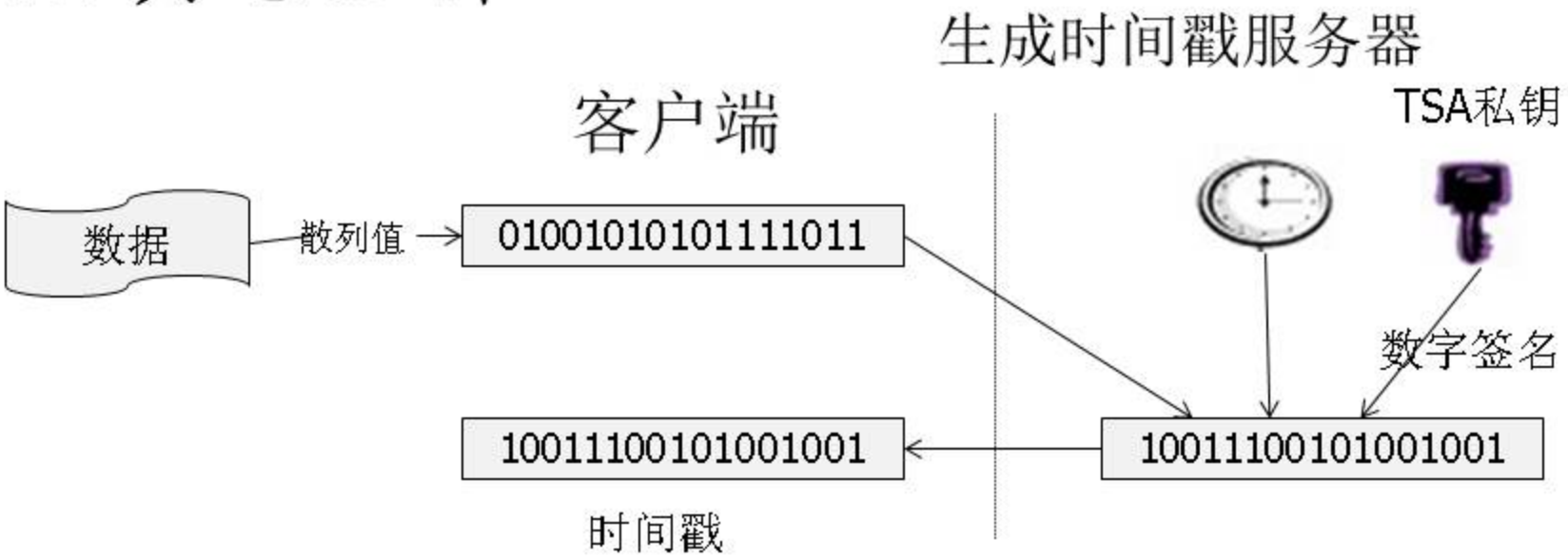

A
B
x
y
$g_a = g^x \pmod p$
g_a
$g_b = g^y \pmod p$
$K = g_a^y \bmod p$
$E_B = E_K(Sig_B(g^x \bmod p, g^y \bmod p))$
检查C(B)
计算 $K = g_a^y \bmod p$
$C(B)$ g_b E_B
解密E_B
验证签名$Sig_B(g^x \bmod p, g^y \bmod p)$
计算
$C(A)$ E_A
检查C(A)
解密E_A
$E_A = E_K(Sig_A(g^x \bmod p, g^y \bmod p))$
验证签名 $Sig_A(g^x \bmod p, g^y \bmod p)$

PKI其它组件

时间戳服务就是时间戳协议（TSP Time Stamp Protocol）通过时间戳（Time Stamp Authority）的服务来提供数据在特定时间存在的证据。

TSA(Time Stamp Authority)，时间戳权威，是一个可信的第三方时间权威。它是PKI 中的重要组成部分。

PKI其它组件



TSA的工作流程：

1. 客户端首先计算所选文件的数字指纹，通常是做一次Hash .
2. 客户端将对文件计算的 Hash 值发送给 TSA ，TSA 将当前时间值加入数字指纹，然后用私有密钥对这个信息数字签名，并产生一个时间邮戳(Time stamp)。
3. TSA 将时间邮戳返回到客户端存储（客户端需要验证时间邮戳的有效性）。这样时间邮戳就跟文件绑在一起作为文件在某个时间内有效的证据。

本节主要内容

- 密钥管理简介
- 密钥分配
- 密钥协商
- PKI及数字证书简介
- **秘密共享**
- 密钥托管

秘密共享

- 秘密共享方案包含三个算法：
  - 参数选取：根据安全策略选成员个数n和门限值t;
  - 秘密分割：将秘密S分为n个子共享$s_1, s_2, \cdots s_n$，并分别秘密分配给n个成员；
  - 秘密恢复：输入至少t个子共享，输出秘密S.

Shamir门限方案

1979年Shamir基于多项式的拉格朗日插值公式提出了一个(t, n)门限方案

秘密共享

（1）参数选取

- 设秘密是S，参与保管的成员共有n个，要求重构该消息需要至少t个人；
- 选定一个足够大的素数p，$p>n$.

秘密共享

（2）秘密分割

- 随机地选定t-1个系数$c_1, c_2, \ldots c_{t-1} \in Z_p$，得到多项式：

$$f(x) \equiv S + c_1 x + \cdots + c_{t-1} x^{t-1} (\mathrm{mod}\ p)$$

- 随机选定n个不同的小于p的整数

例如：$1, 2, 3, \cdots, n$

对于每个整数x_i分别计算数对$s_i=(x_i,y_i)$,

$$y_i \equiv f(x_i) (\mathrm{mod}\ p)$$

- 销毁多项式，并将n个子共享$\{s_i=(x_i,y_i) \mid i=1,2,\ldots,n\}$分别秘密传送给$n$个成员。

秘密共享

（3）秘密恢复

假设个人聚集准备恢复秘密，不妨设他们持有的子共享分别为 $s_1 = (x_1, y_1), \ldots, s_t = (x_t, y_t)$.

- t个人共同计算多项式

$$f(x) \equiv \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j \neq k}}^{t} \frac{x - x_j}{x_k - x_j} (\mathrm{mod}\ p)$$

- 取多项式$f(x)$的常数项$f(0)$即为所求秘密S.

秘密共享

（4）实例

秘密是S=120114070608

①参数选取

- 选取n=5个成员保管秘密，要求至少t=3个人联合才能够重构秘密，即创建一个(3,5)门限方案。
- 选定一个足够大的素数p=1234567890133，满足$p>n$.

秘密共享

② 随机地选定2个系数，得到多项式：

$$f(x) = 120114070608 + 1206749628665x + 482943028839x^2$$

- 随机选定5个小于p的整数，例如：1,2,3,4,5.
  对于每个整数x_i分别计算 $y_i \equiv f(x_i) (\mathrm{mod}\ p)$

$$\begin{pmatrix} 1, & 575238837979 \\ 2, & 761681772895 \\ 3, & 679442875356 \\ 4, & 328522145362 \\ 5, & 943487473046 \end{pmatrix}$$

- 销毁多项式，并将5个子共享$\{s_i=(x_i,y_i) | i=1,2,\ldots,5\}$分别秘密传送给5个成员。

秘密共享

③秘密恢复

假设3个人恢复秘密，不妨设他们持有的子共享为

(1, 575238837979), (3, 679442875356), (5, 943487473046)

- t个人共同计算多项式

$$f(x) \equiv (575238837979\frac{(x-3)(x-5)}{(1-3)(1-5)} + 679442875356\frac{(x-1)(x-5)}{(3-1)(3-5)} + 943487473046\frac{(x-1)(x-3)}{(5-1)(5-3)}) \bmod p$$

$$\equiv (575238837979\frac{(x-3)(x-5)}{8} - 679442875356\frac{(x-1)(x-5)}{4} + 471743736523\frac{(x-1)(x-3)}{4}) \bmod p$$

秘密共享

③秘密恢复

- t个人共同计算多项式

$$f(x) \equiv (482943028839x^2 + 1206749628665x + 120114070608) \bmod p$$

- 取多项式$f(x)$的常数项$f(0)$即为所求秘密S.

本节主要内容

- 密钥管理简介
- 密钥分配
- 密钥协商
- PKI及数字证书简介
- 秘密共享
- 密钥托管

密钥托管

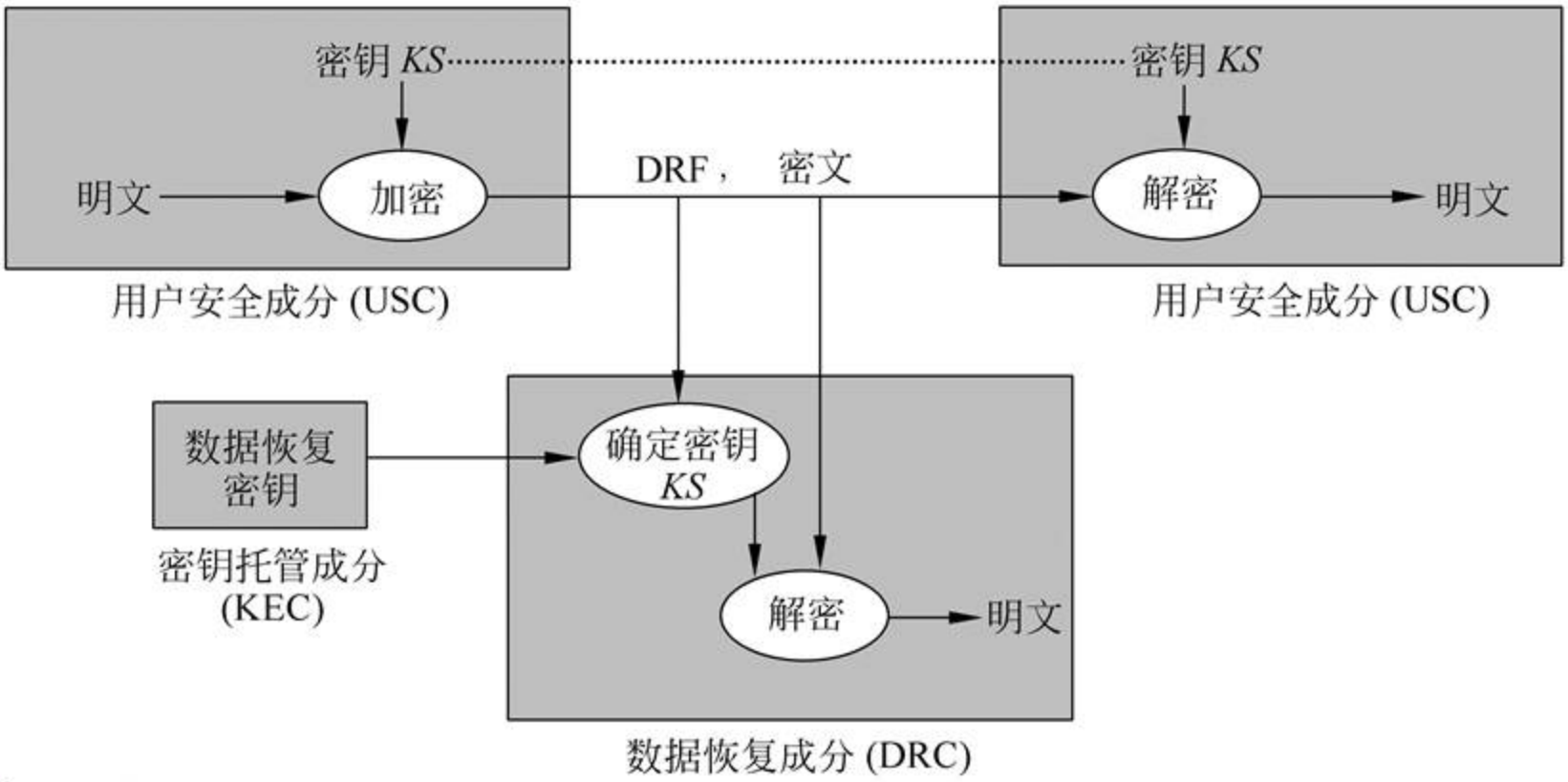
目的：为了有效控制密码技术的使用，保证对个人没有绝对的隐私和绝对不可跟踪的匿名性。

用途：提供一个备用的解密途径，政府机构在需要时，可通过密钥托管技术解密用户的信息，而用户的密钥若丢失或损坏，也可通过密钥托管技术恢复自己的密钥。

起源：美国政府于1993年4月提出Clipper计划，建议联邦政府和工业界使用新的具有密钥托管功能的托管加密标准EES（Escrowed Encryption Standard）。EES标准于1994年2月正式被美国政府公布采用。

密钥托管

密钥托管密码体制的组成



密钥托管

密钥托管密码体制组成：

（1）用户安全成分USC（user security component）

- 作用：提供数据加解密能力以及支持密钥托管功能；
- USC可用于通信和数据存储的密钥托管；
- USC使用的加密算法可以是保密的、专用的，也可以是公钥算法。

密钥托管

（2）密钥托管成分KEC (key escrow component)

- 作用：存储所有的数据恢复密钥，通过向DRC提供所需的数据和服务以支持DRC。
- 托管代理机构也为可信赖的第三方，需要在密钥托管中心注册。
- 职责：操作KEC，协调托管代理机构的操作或担当USC或DRC的联系点

密钥托管

（3）数据恢复成分DRC (data recovery component)

- 作用：由KEC提供的用于通过密文及DRF中的信息获得明文的算法、协议和仪器。
- 它仅在执行指定的已授权的恢复数据时使用。

本节要点回顾

- PKI及数字证书简介
  - 公钥的分发问题
  - PKI简介
  - 证书管理
  - PKI其它组件

THE END!