密 码 学

第十六讲　密钥管理:

王后珍

武汉大学国家网络安全学院

空天信息安全与可信计算教育部重点实验室

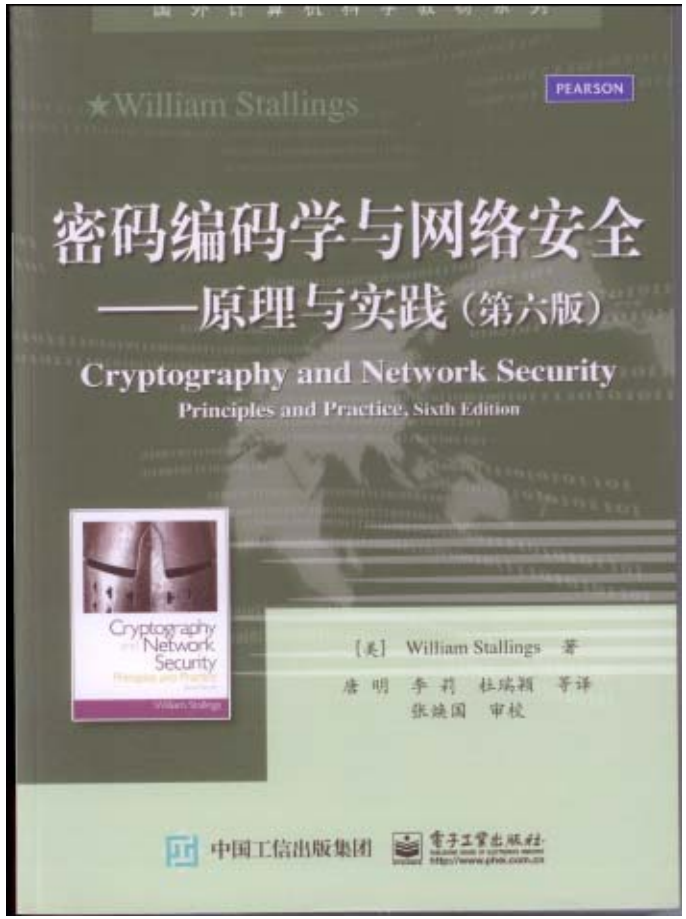
目 录

目 录

教材与主要参考书

教材

参考书



本讲内容

一、密钥管理的概念

二、密钥管理的原则

三、对称密码的密钥管理

一、密钥管理的概念

- 密码的公开设计原则：

  密码体制的安全应当只取决于密钥的安全，而不取决与对密码算法的保密。

- 密钥管理包括密钥的产生、存储、分配、组织、使用、停用、更换、销毁等一系列技术问题。

- 每个密钥都有其生命周期，要对密钥的整个生命周期的各个阶段进行全面管理。

- 密码体制不同，密钥的管理方法也不同。

一、密钥管理的概念

- 密钥管理是一个很困难的问题。
- 历史表明，从密钥管理环节窃取秘密，要比单纯从破译密码算法窃取秘密所花的代价小得多。
- 在密码算法确定之后，密钥管理就成为密码应用中最重要的问题！

二、密钥管理的原则

- 区分密钥管理的策略和机制
  - 策略是密钥管理系统的高级指导。策略重在原则指导，而不重在具体实现。策略通常是原则的、简单明确的。
  - 机制是实现和执行策略的技术和方法。机制是具体的、复杂繁琐的。
  - 没有好的管理策略，再好的机制也不能确保密钥的安全。相反，没有好的机制，再好的策略也没有实际意义。
- 全程安全原则
  - 必须在密钥的产生、存储、分配、组织、使用、停用、更换、销毁的全过程中对密钥采取妥善的安全管理。只有各个阶段都是安全时，密钥才是安全的。
  - 密钥从一产生到销毁的全过程中除了在使用的时候可以以明文形式出现外都不应当以明文形式出现。

二、密钥管理的原则

- 最小权利原则
  - 应当只分配给用户进行某一事务处理所需的最小的密钥集合。
- 责任分离原则
  - 一个密钥应当专职一种功能，不要让一个密钥兼任几个功能。 例如，用于加密的密钥不能用于签名。
- 密钥分级原则
  - 对于一个大的系统，应当采用密钥分级的策略。
  - 根据密钥的职责和重要性，把密钥划分为几个级别。
  - 用高级密钥保护低级密钥，最高级的密钥由物理、技术和管理安全保护。
  - 这样，既可减少受保护的密钥的数量，又可简化密钥的管理工作。

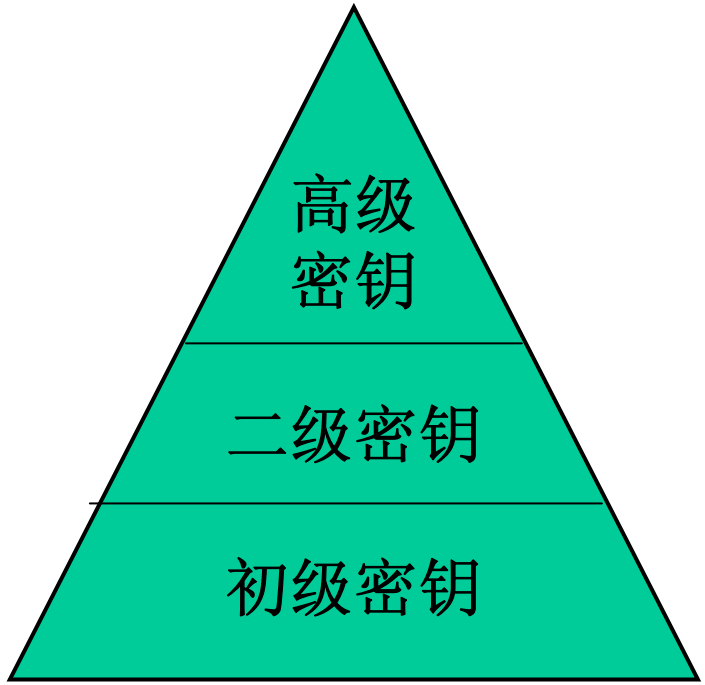
二、密钥管理的原则

- 密钥更换原则。
  - 密钥必须按时更换。否则，即使是采用很强的密码算法，时间越长，被破译的可能性就越大。
  - 理想情况是一个密钥只使用一次，但是完全的一次一密是不现实的。
  - 一般，初级密钥采用一次一密，中级密钥更换的频率低些，主密钥更换的频率更低些。
  - 密钥更换的频率越高，越有利于安全，但是密钥的管理就越麻烦。实际应用时应当在安全和方便之间折衷。

三、传统密码的密钥管理

1、密钥组织

- 将密钥分为三级：
  - 初级密钥
  - 二级密钥
  - 主密钥 (高级密钥)



三、传统密码的密钥管理

①初级密钥

- 我们称直接用于加解密数据(通信、文件)的密钥为初级密钥，记为K。
  - 称用于通信保密的初级密钥为初级通信密钥，记为K_c。
  - 称用于保护会话的初级密钥为会话密钥(Session Key)，记为K_s。
  - 称用于文件保密的初级密钥为初级文件密钥(File Key)，记为K_f。

三、传统密码的密钥管理

①初级密钥

- 初级密钥可通过硬件或软件方式自动产生，也可由用户自己提供。
- 初级通信密钥和初级会话密钥原则上采用一个密钥只使用一次的“一次一密”方式。
- 初级通信密钥的生存周期很短。
- 初级文件密钥与所保护的文件的生存周期一样长。
- 初级密钥必须受更高一级的密钥保护，直到它们的生存周期结束为止。

三、传统密码的密钥管理

②二级密钥

- 二级密钥(Secondary Key)用于保护初级密钥，记作K_N，这里N表示节点，源于它在网络中的地位。
- 当二级密钥用于保护初级通信密钥时称为二级通信密钥，记为K_{NC}。
- 当二级密钥用于保护初级文件密钥时称为二级文件密钥，记为K_{NF}。

三、传统密码的密钥管理

②二级密钥

- 二级密钥的安装
  - 可由专职密钥安装人员提供并安装。
  - 也可经专职密钥安装人员批准，由系统自动产生。
  - 二级密钥的生存周期一般较长，它在较长的时间内保持不变。
- 二级密钥必须接受高级密钥的保护。

三、传统密码的密钥管理

③主密钥

- 主密钥(Master Key)是密钥管理方案中的最高级密钥，记作K_M。
- 主密钥用于对二级密钥和初级密钥进行保护。
- 主密钥由密钥专职人员产生，并妥善安装。
- 主密钥的生存周期很长。
- 主密钥只能以明文形式存储。
- 必须采用安全的物理、技术、管理措施对主密钥进行保护！

三、传统密码的密钥管理

2、密钥产生

- 对密钥的一个基本要求是要具有良好的安全性：随机性、非线性、等概性以及不可预测性等。
- 一个真正的随机序列是不可以人为控制再现的。任何人都不能人为地控制再次产生它。
  - 有限长度的随机序列会重复，但不能人为控制重复。
  - 任何算法产生的随机数都不是真随机的，因为可人为控制重复。
- 高效地产生高质量的真随机序列，并不是一件容易的事。

三、传统密码的密钥管理

2、密钥产生

①主密钥的产生

- 主密钥应当是高质量的真随机序列。真随机数应该从自然界的随机现象中提取。
  - ■基于力学噪声源的密钥产生
  - ■基于电子学噪声源的密钥产生
  - ■基于量子力学噪声源的密钥产生
- 要经过严格的随机性测试。

三、传统密码的密钥管理

2、密钥产生

②二级密钥的产生

- 可以象产生主密钥那样产生真随机的二级密钥。
- 在主密钥产生后，也可借助于主密钥和一个强的密码算法来产生二级密钥。
- 设RN_1和RN_2是真随机数，RN_3是随机数，然后分别以它们为密钥对一个序数进行四层加密，产生出二级密钥K_N。

$$K_N = E(E(E(E(i, RN_1), RN_2), RN_1), RN_3)$$

- 要想根据序数i预测出密钥K_N，必须同时知道两个真随机数RN_1，RN_2和一个随机数RN_3，这是极困难的。

三、传统密码的密钥管理

2、密钥产生

③初级密钥的产生

- 为了安全和简便，通常总是把随机数*RN*直接视为受高级密钥加密过的初级密钥：

$$RN=E(K_s,\ K_M)\ \text{或}\ RN=E(K_f,\ K_M),$$

$$RN=E(K_s,\ K_{NC})\ \text{或}\ RN=E(K_f,\ K_{NF})。$$

- 使用初级密钥时，用高级密钥将随机数RN解密：

$$K_s=D(RN,\ K_M)\quad \text{或}\ K_f=D(RN,\ K_M),$$

$$K_s=D(RN,\ K_{NC})\ \text{或}\ K_f=D(RN,\ K_{NF})$$

- 好处：安全，一产生就是密文，方便。

三、传统密码的密钥管理

2、密钥产生

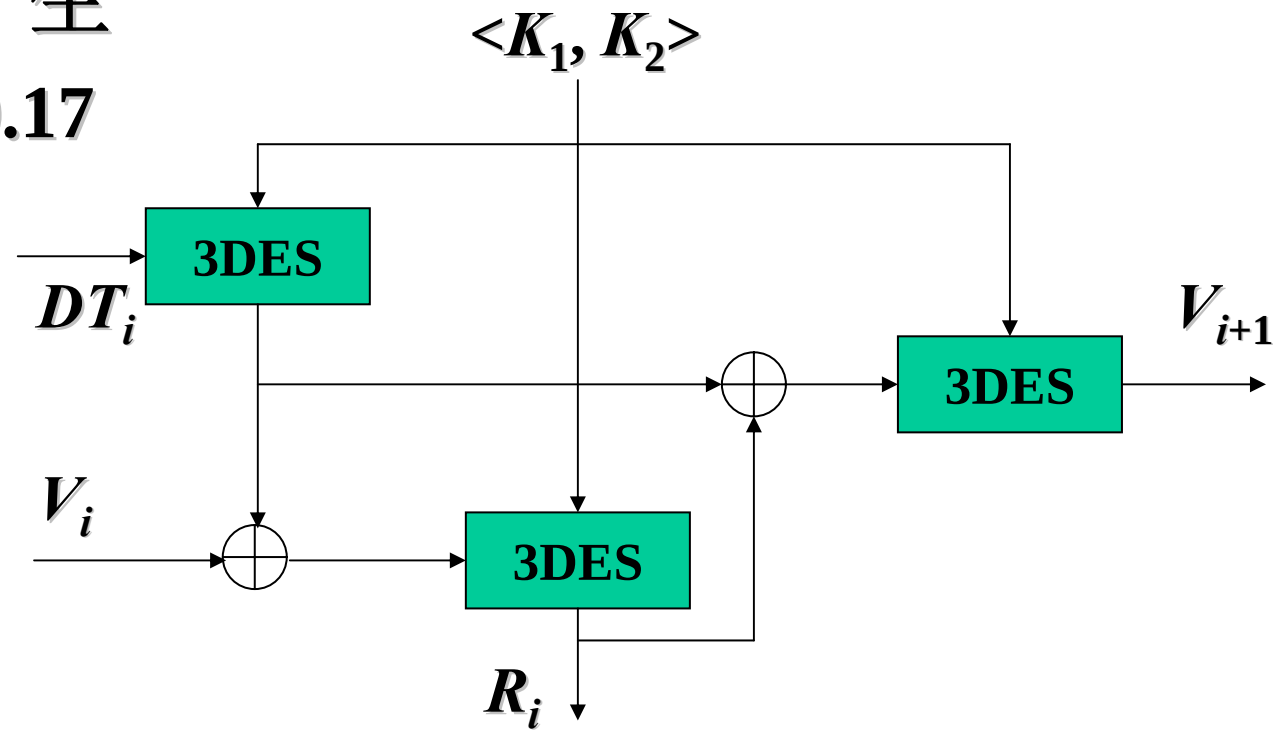
④伪随机数的产生

- 二级密钥和初级密钥的产生都需要伪随机数。
- 伪随机性：随机，长周期，独立性，非线性
- 一般采用基于强密码算法的产生方法

三、传统密码的密钥管理

2、密钥产生

- ANSI X9.17

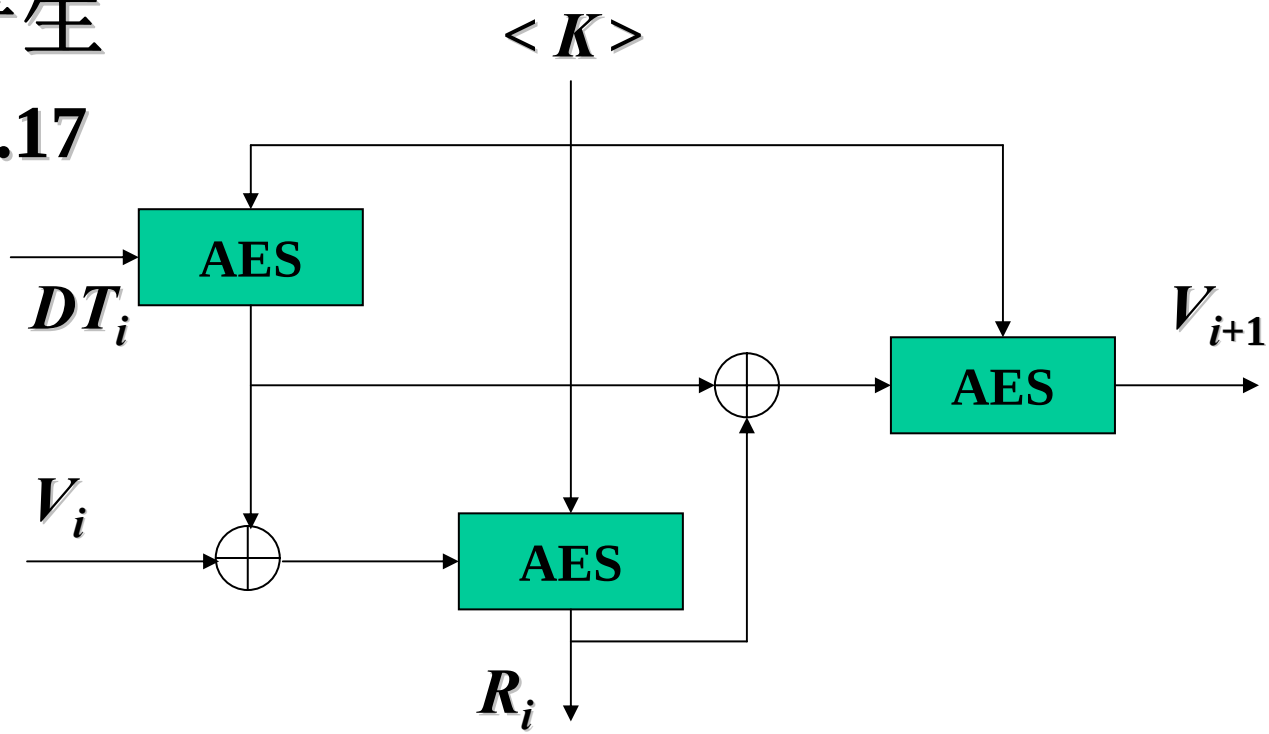


- 用作美国电子支付标准，因特网的PGP也采用。

三、传统密码的密钥管理

2、密钥产生

- ANSI X9.17



AES方案

三、传统密码的密钥管理

2、密钥分配

- 密钥分配自古以来就是密钥管理中重要而薄弱的环节。
- 过去，密钥的分配主要采用人工分配。
- 现在，应当利用计算机网络实现密钥分配的自动化。

①主密钥的分配

- 一般采用人工分配主密钥，由专职密钥分配人员分配并由专职安装人员妥善安装。

三、传统密码的密钥管理

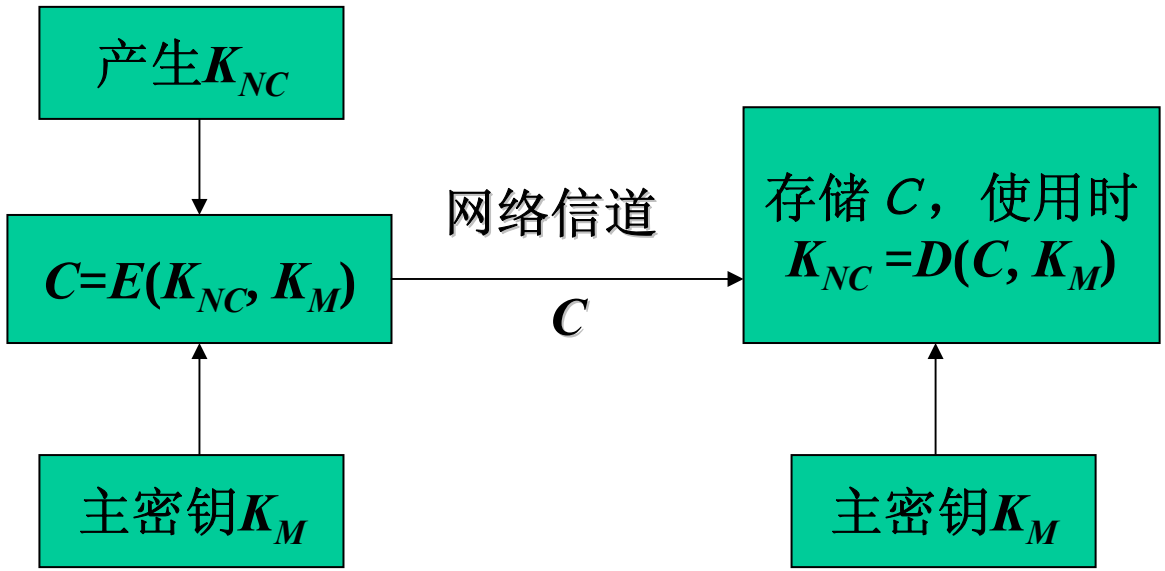
2、密钥分配

②二级密钥的分配

- 一种方法是，由专职密钥分配人员分配并由专职安装人员安装。虽然这种人工分配和安装的方法很安全，但是效率低，成本高。
- 另一种方法的原理是，直接利用已经分配安装的主密钥对二级密钥进行加密保护，并利用计算机网络自动传输分配。

三、传统密码的密钥管理

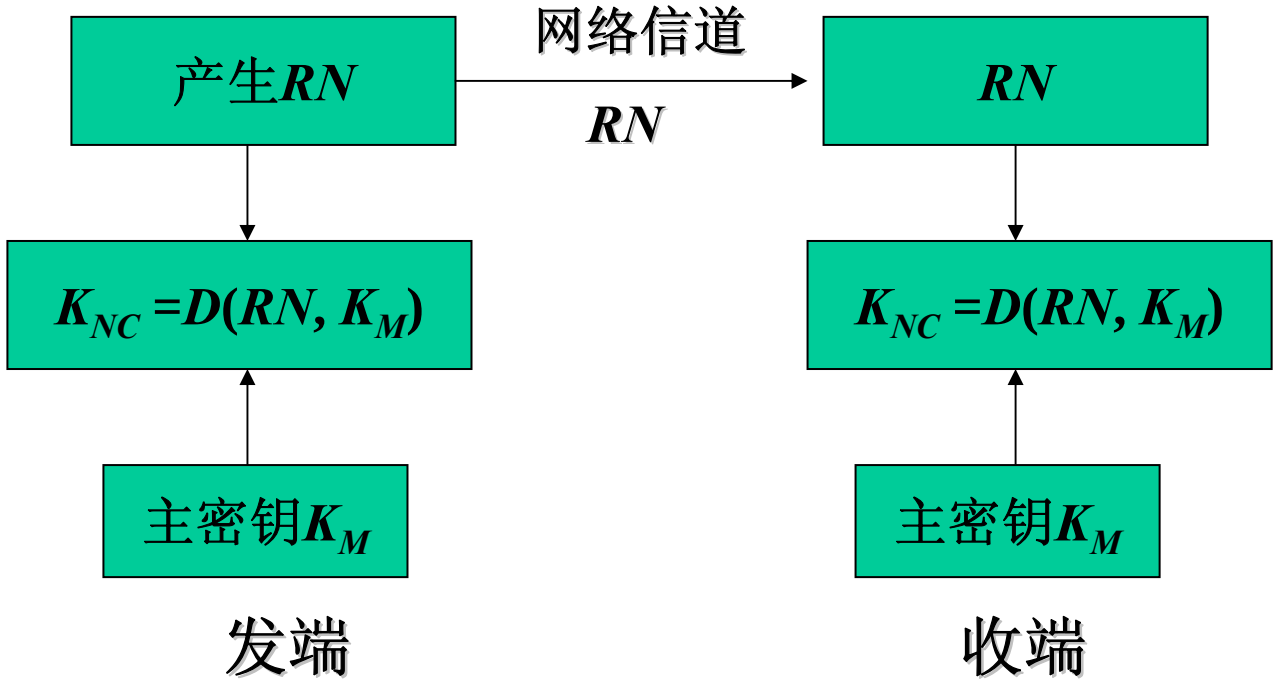
2、密钥分配



方案1原理图

三、传统密码的密钥管理

2、密钥分配



方案2原理图

三、传统密码的密钥管理

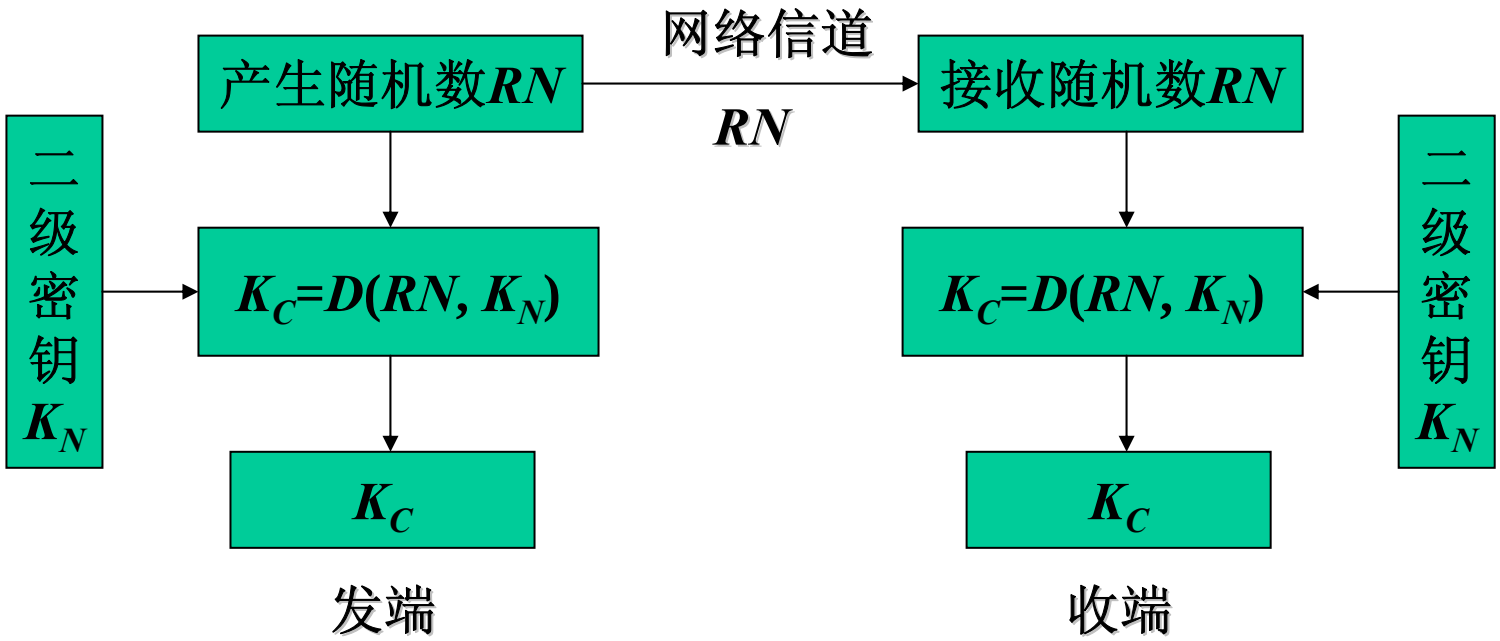
2、密钥分配

③初级密钥的分配

- 通常总是把一个随机数直接视为受高级密钥（主密钥或二级密钥，通常是二级密钥）加密过的初级密钥，这样初级密钥一产生便成为密文形式。
- 发端直接把密文形式的初级密钥通过计算机网络传给收方，收端用高级密钥解密便获得初级密钥。

三、传统密码的密钥管理

2、密钥分配



原理图

武漢大学

$y_A = \alpha^{x_A} \bmod p$

三、传统密码的密钥管理

2、密钥分配

- **Diffie-Hellman密钥分配协议**

① 选择一个大素数p和$GF(p)$的一个本原元α，p和α为系统所有用户所共享。

② 用户A选择一个随机整数$1<x_A<p$，以x_A作为自己的私钥，以 $y_A = \alpha^{x_A} \bmod p$ 作为自己的公钥。A发公钥y_A给B。

③ 用户B选择一个随机整数$1<x_B<p$，以x_B作为自己的私钥，以 $y_B = \alpha^{x_B} \bmod p$ 作为自己的公钥。B发公钥y_B给A。

④ 用户A收到y_B后，计算 $K_A = (y_B)^{x_A} \bmod p$，并将$K_A$作为密钥。用户B收到$y_A$后，计算 $K_B = (y_A)^{x_B} \bmod p$，并将$K_B$作为密钥。显然$K_A = K_B$，A和B共享了密钥。

三、传统密码的密钥管理

2、密钥分配

- **Diffie-Hellman密钥分配协议**
  - ■密钥分配正确性

$K_A = K_B$，这是因为，

$$K_A = (y_B)^{x_A} \bmod p = (\alpha^{x_B})^{x_A} \bmod p = (\alpha^{x_A})^{x_B} \bmod p = (y_A)^{x_B} = K_B$$

三、传统密码的密钥管理

2、密钥分配

- **Diffie-Hellman密钥分配协议**
  - 安全性
  - 攻击一：截获 $y_A = \alpha^{x_A} \bmod p$ 和 $y_B = \alpha^{x_B} \bmod p$，求出私钥 x_A 和 x_B。但需要求解离散对数问题，这是困难的。
  - 攻击二：通过截获的 y_A 和 y_B 直接求出密钥 $K = \alpha^{x_A x_B} \bmod p$，问题的困难性尚未被证明，人们普遍认为它是困难的，并把这一观点称为**Diffie-Hellman假设**。
  - 中间人攻击：攻击者冒充A与B联系获得一个共享密钥、冒充B与A联系获得一个共享密钥，从而获得A和B之间的信息。攻击性像位于A和B中间的一个“二传手”，所以称为中间人攻击。

二、中国商用公钥密码SM2签名算法

2、 密钥分配

- 中国商用密码SM2密钥分配协议
  - 推荐使用256位素域$GF(p)$上的椭圆曲线：

$$y^2 = x^3 + ax + b$$

p = 8542D69E 4C044F18 E8B92435 BF6FF7DE 45728391 5C45517D 722EDB8B 08F1DFC3
a = 787968B4 FA32C3FD 2417842E 73BBFEFF 2F3C848B 6831D7E0 EC65228B 3937E498
b = 63E4C6D3 B23B0C84 9CF84241 484BFE48 F61D59A5 B16BA06E 6E12D1DA 6E12D1DA
n = 8542D69E 4C044F18 E8B92435 BF6FF7DD 29772063 0485628D 5AE74EE7 C32E79B7
h=1
Gx = 421DEBD6 1B62EAB6 746434EB C3CC315E 32220B3B ADD50BDC 4C4E6C14 7FEDD43D
Gy = 0680512B CBB42C07 D47349D2 153B70C4 E5D7FDFC BFA36EA1 A85841B9 E46E09A2

  - 用户密钥：
    - 私钥是随机数：d，$d \in [1, n-1]$
    - 公钥是点：$P = dG$

三、传统密码的密钥管理

2、密钥分配

- 中国商用密码SM2密钥分配协议
  - 设A的私钥为d_A，公钥为$P_A = d_A G = (x_A, y_A)$，B的私钥为d_B，公钥为$P_B = d_A G = (x_B, y_B)$。
  - 设A的标识符为ID_A，长度为entlen_A比特。记$ENTL_A$是由整数entlen_A转换而成的两个字节。B的标识符为ID_B，长度为entlen_B比特。记$ENTL_B$是由整数entlen_B转换而成的两个字节。
  - 设A的杂凑值Z_A和B的杂凑值Z_B，
  - $Z_A = \text{SM3}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$;
  - $Z_B = \text{SM3}(ENTL_B \| ID_B \| a \| b \| x_G \| y_G \| x_B \| y_B)$。
  - 记$w = \lceil (\lceil \log_2(n) \rceil / 2) \rceil - 1$。

三、传统密码的密钥管理

- 中国商用密码SM2密钥分配协议

A执行以下步骤：

① 产生随机数 $r_A \in [1, n-1]$；

② 计算椭圆曲线点 $R_A = r_A \cdot G = (x_1, y_1)$；

③ 将 R_A 发送给B；

④ 从 R_A 中取出分量 x_1，将其数据类型转换为整数，并计算 $XX_1 = 2^w + (x_1 \& (2^w - 1))$；

⑤ 计算 $t_A = (d_A + XX_1 \cdot r_A) \bmod n$；

⑥ 接收B发来的 R_B。验证 R_B 是否满足曲线方程，若不满足则协商失败退出；否则从 R_B 中取出分量 x_2，将其数据类型转换为整数，计算 $XX_2 = 2^w + (x_2 \& (2^w - 1))$；

⑦ 计算点 $U = (h \cdot t_A)(P_B + XX_2 \cdot R_B) = (x_U, y_U)$，若 U 是无穷远点，则A协商失败退出；否将 x_U、y_U 的数据类型转换为比特串；

⑧ 计算 $K_A = KDF(x_U \| y_U \| Z_A \| Z_B, klen)$；至此，用户A获得密钥 K_A。

三、传统密码的密钥管理

- 中国商用密码SM2密钥分配协议

B执行以下步骤：

① 产生随机数 $r_B \in [1, n-1]$；

② 计算椭圆曲线点 $R_B = r_B \bullet G = (x_2, y_2)$；

③ 将 R_B 发送给A；

④ 从 R_B 中取出分量 x_2，将其数据类型转换为整数，并计算 $XX_2 = 2^w + (x_2 \& (2^w - 1))$；

⑤ 计算 $t_B = (d_B + XX_2 \bullet r_B) \bmod n$；

⑥ 接收A发来的 R_A。验证 R_A 是否满足曲线方程，若不满足则协商失败退出；否则从 R_A 中取出分量 x_1，将其数据类型转换为整数，计算 $XX_1 = 2^w + (x_1 \& (2^w - 1))$；

⑦ 计算点 $V = (h \bullet t_B)(P_A + XX_1 \bullet R_A) = (x_V, y_V)$，若 V 是无穷远点，则B协商失败退出；否将 x_V、y_V 的数据类型转换为比特串；

⑧ 计算 $K_B = KDF(x_V \| y_V \| Z_A \| Z_B, klen)$；至此，用户B获得密钥 K_B。

三、传统密码的密钥管理

2、密钥分配

- 中国商用密码SM2密钥分配协议
  - 正确性
  - ◆ 要证明$K_A=K_B$，只需证明$U(x_U, y_U)=V(x_V, y_V)$。
  - ◆ 一方面，$V=(h\cdot t_B)(P_A+XX_1 R_A)=(h\cdot t_B)(d_A\cdot G+XX_1 r_A\cdot G)=(h\cdot t_B)(d_A+XX_1 r_A)G=[h\cdot(d_B+XX_2\cdot r_B)](d_A+XX_1 r_A)G=(h\cdot G)[d_B d_A+XX_2\cdot r_B d_A+d_B XX_1 r_A+XX_2\cdot r_B XX_1 r_A]$。
  - ◆ 另一方面，$U=(h\cdot t_A)(P_B+XX_2\cdot R_B)=(h\cdot t_A)(d_B\cdot G+XX2 r_B\cdot G)=(h\cdot t_A)(d_B+XX_2 r_B)G=[h\cdot(d_A+XX_1\cdot r_A)](d_B+XX_2 r_B)G=(h\cdot G)[d_A d_B+XX_1\cdot r_A d_B+d_A XX_2 r_B+XX_1\cdot r_A XX_2 r_B]$。
  - ◆ 可见，$U(x_U, y_U)=V(x_V, y_V)$。

三、传统密码的密钥管理

2、密钥分配

- 中国商用密码SM2密钥分配协议
  - 安全性
    - 由公钥$P = dG = (x, y)$求私钥d，要求解ECDLP问题。这是困难的。
    - 计算共享密钥需要计算点U和V，其中要用私钥d，攻击者没有d，所以攻击是困难的。
    - 在协商所得密钥中包含了用户A和B的身份标识信息、曲线参数信息。这对提高了安全性起到一定的作用。
    - 与SM2的其他算法一样，密钥交换协议也采用了许多检错措施。这不仅提高了协议的数据完整性和系统可靠性，而且也提高了协议的安全性。
    - 从应用看来，这一协议与DH协议相比，比较复杂。如果能够更加简明，则用户应用将会更方便。

三、传统密码的密钥管理

3、密钥的存储

- 密钥的安全存储就是要确保密钥在存储状态下的秘密性、真实性和完整性。
- 安全可靠的存储介质是密钥安全存储的物质条件，安全严密的访问控制是密钥安全存储的管理条件。
- 密钥安全存储的原则是不允许密钥以明文形式出现在密钥管理设备之外。

三、传统密码的密钥管理

3、密钥的存储

- 密钥的存储形态有以下几种：
  - 明文形态：明文形式的密钥。
  - 密文形态：被密钥加密密钥加密过的密钥。
  - 分量形态：密钥分量不是密钥本身，而是用于产生密钥的部分参数。

三、传统密码的密钥管理

3、密钥的存储

①主密钥的存储

- 主密钥是最高级的密钥，所以它只能以明文形态存储，否则便不能工作。
- 要求存储器必须是物理上高度安全的，而且访问控制上也是高度安全的。
- 通常是将其存储在专用密码装置中。

三、传统密码的密钥管理

3、密钥的存储

②二级密钥的存储

- 二级密钥可以以被主密钥加密的密文形态存储。
- 且要求存储器必须是高度安全的（物理上和访问控制上）。
- 这样可减少明文形态密钥的数量，便于管理。

三、传统密码的密钥管理

3、密钥的存储

③初级密钥的存储

- 初级文件密钥和初级会话密钥是两种性质不同的初级密钥，因此其存储方式也不相同。
- 初级文件密钥的生命周期与受保护的文件的生命周期一样长。因此初级文件密钥需要妥善的存储。
- 初级文件密钥一般采用密文形态存储，通常采用以二级文件密钥加密的形式存储初级文件密钥。
- 初级会话密钥按“一次一密”的方式工作，使用时动态产生，使用完毕后即销毁，生命周期很短。因此，初级会话密钥的存储空间是工作存储器，应当确保工作存储器的安全。

三、传统密码的密钥管理

4、密钥的更新

- 当密钥的使用期限已到，或怀疑密钥泄露时密钥必须更新。
- 密钥的更新是密钥管理中非常麻烦的一个环节。

① 高级密钥的更新

- 必须重新产生并安装，其安全要求与其初次产生安装一样。
- 高级密钥的更新将导致受其保护的中级密钥和初级密钥都要更新。

三、传统密码的密钥管理

4、密钥的更新

② 二级密钥的更新

- 安全要求与其初次产生安装时一样。
- 二级密钥的更新也将要求受其保护的初级密钥也更新。

③ 初级密钥的更新

- 初级会话密钥采用一次一密的方式工作，因此更新是极容易的。
- 初级文件密钥更新时，必须将原来的密文文件解密并用新的初级文件密钥重新加密。

三、传统密码的密钥管理

5、密钥的终止和销毁

- 这一环节往往容易被忽视。
- 当密钥的使用期限到期时，必须终止使用该密钥，并更换新密钥。
- 终止使用的密钥，并不立即销毁，而需要再保留一段时间然后再销毁。这是为了确保受其保护的其他密钥和数据得以妥善处理。只要密钥尚未销毁，就必须对其进行保护。
- 密钥销毁要彻底清除密钥的一切存储形态和相关信息，使得恢复这一密钥成为不可能。
- 要采用妥善的清除存储器的方法。对于磁记录存储器，简单地删除、清0或写1都是不安全的。

目 录

目 录

本讲内容

一、公钥密码密钥管理的概念

二、公钥密码的密钥产生

三、公钥密码的密钥分配

四、公钥证书的概念

五、公钥基础设施PKI

一、公钥密码密钥管理的概念

- 密码体制不同，密钥的管理方法也不同。因此公钥密码的密钥管理与传统密码的密钥管理大不相同：
- 传统密码只有一个密钥，加密钥等于解密钥（$K_e = K_d$）。因此，密钥的秘密性、真实性和完整性都必须保护。
- 公开密钥密码有两个密钥，加密钥与解密钥不同（$K_e \neq K_d$），而且由加密钥在计算上不能求出解密钥，所以加密钥的秘密性不用确保。

一、公钥密码密钥管理的概念

- 虽然公开密钥密码体制的加密钥可以公开，其秘密性不需要保护，但其完整性和真实性却必须严格保护。
- 公开密钥密码体制的解密钥的秘密性、真实性和完整性都必须保护。

二、公钥密码的密钥产生

- 传统密码体制的密钥本质上是一种随机数或随机序列，因此传统密码体制的密钥产生本质上是产生具有良好密码学特性的随机数或随机序列。

- 公开密钥密码体制本质上是一种单向陷门函数，它们都是建立在某一数学难题之上的。不同的公开密钥密码体制所依据的数学难题不同，因此其密钥产生的具体要求不同。但是，它们都必须满足密码安全性和应用的有效性对密钥所提出的要求。

二、公钥密码的密钥产生

1. RSA密码的密钥产生

- 对于**RSA**密码，其秘密解密密钥为<$p,q,\phi(n),d$>，公开加密钥为<n,e>，因此其密钥的产生主要是根据安全性和工作效率来合理的产生这些密钥参数。
- p和q越大则越安全，但工作效率就越低。反之，p和q越小则工作效率就越高，但安全性就越低。根据目前的因子分解能力，对于一般应用，p和q至少要有**512**位，以使**n**至少有**1024**位；而对于重要应用，p和q至少要有**1024**位，以使n至少有**2048**位。p和q要随机；p和q的差要大；（$p-1$）和（$q-1$）的最大公因子要小；e和d都不能太小；等等。

二、公钥密码的密钥产生

2. 椭圆曲线密码的密钥产生

- 椭圆曲线密码，由下面的六元组所描述：

$$T=<p,a,b,G,n,h>$$

其中，p为大素数，p确定了有限域$GF(p)$；元素$a,b \in GF(p)$，a和b确定了椭圆曲线；G为循环子群E_1的生成元，n为素数且为生成元G的阶。

- 私钥定义为一个随机数d，

$d \in \{0,1,2,\cdots,n-1\}$，$d$既不能太小，也不能太大。

- 公钥定义为Q点，

$Q=dG$ 。

二、公钥密码的密钥产生

- 对于椭圆曲线密码，其用户的私钥d和公钥Q的生成并不困难。
- 困难的是其系统参数$<p,a,b,G,n>$的选取。也就是椭圆曲线的选取。
- 美国NIST推荐了15条椭圆曲线。
- 中国的商用密码SM2使用了自己的椭圆曲线。
- 我们用演化密码的方法产生了大量的椭圆曲线。
- 目前椭圆曲线的参数n和p的规模应大于2^{160}。
- 参数越大，越安全，但运算越困难，资源消耗也越多。

三、公钥密码的密钥分配

- 和传统密码一样，公钥密码也需要进行密钥分配。但是，公钥密码的密钥分配与传统密码体制的密钥分配有着本质的差别。
- 在密钥分配时必须做到：
  - 因为公钥是公开的，因此不需确保秘密性。但必须确保公钥的真实性和完整性
  - 确保私钥的秘密性、真实性和完整性。

三、公钥密码的密钥分配

- 如果公钥的真实性和完整性受到危害，则基于公钥的各种应用的安全将受到危害。
- 举例：C冒充A欺骗B的攻击方法

①攻击者C在PKDB中用自己的公钥K_{eC}替换用户A的公钥K_{eA}。

②C用自己的解密钥签名一个消息冒充A发给B。

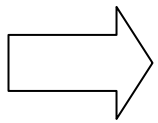
$$C \rightarrow B: <A, D(M, K_{dC})>$$

③B验证签名：因为此时PKDB中A的公开钥已经替换为C的公开钥，故验证为真。

三、公钥密码的密钥分配

PKDB

A	K_{eA}
B	K_{eB}
C	K_{eC}



PKDB

A	K_{eC}
B	K_{eB}
C	K_{eC}

攻击者C篡改PKDB

三、公钥密码的密钥分配

- 结果
  - 因验证签名为真，于是B认为攻击者C就是A。
  - 若B要发送加密的消息给A，则B要用A的公开钥进行加密，但A的公开钥已被换成C的公开钥，因此B实际上是用C的公开钥进行了加密。
  - C从网络上截获B发给A的密文。由于这密文实际上是用C的公开钥加密的，所有C可以解密得到明文。A反而不能正确解密。

三、公钥密码的密钥分配

- 上述攻击成功的原因：

①对存入**PKDB**的公开钥没有采取保护措施，致使公开加密钥被替换而不能发现；

②存入**PKDB**的公开钥与用户的标识符之间没有绑定关系，致使**A**的公钥替换成**C**的公钥后不能发现公开钥与用户的标识符之间的对应关系被破坏。

四、公钥证书的概念

- 采用数字签名技术可以克服上述两个缺点，确保公开加密钥的安全分配。
- 经过可信实体签名的一组信息的集合被称为证书（**Certificate**），而可信实体被称为签证机构 **CA**（**Certification Authority**）。
- 一般地讲，证书是一个数据结构，是一种由一个可信任的权威机构签署的信息集合。
- 在不同的应用中有不同的证书。例如公钥证书**PKC**（**Public Key Certificate**）、**PGP**证书、**SET**证书等。

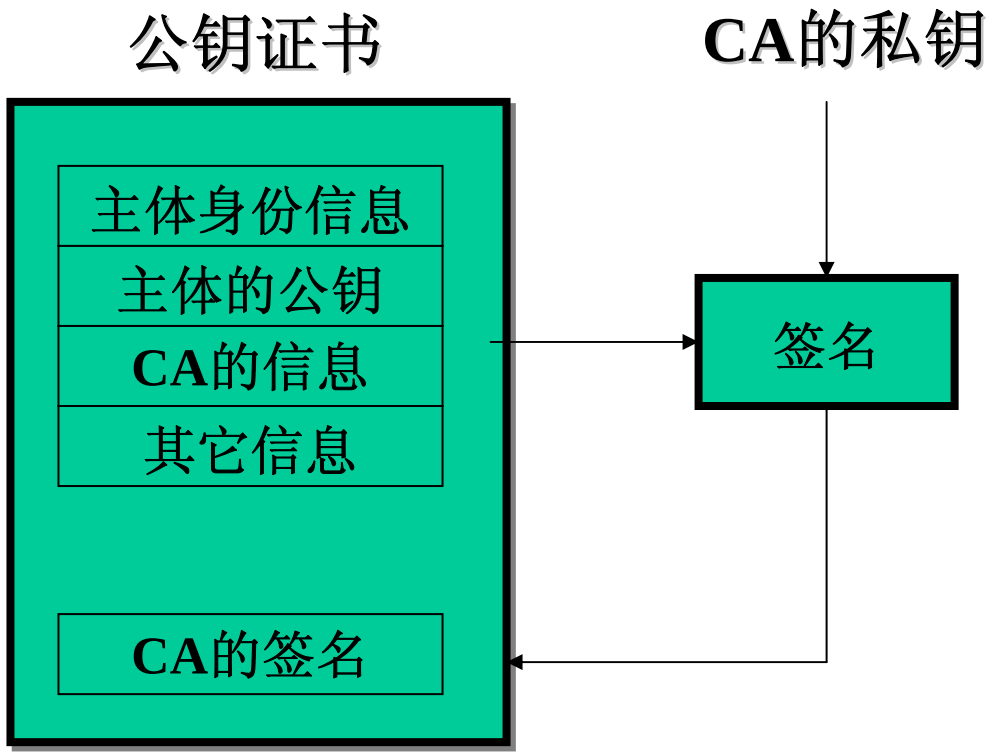
四、公钥证书的概念

- 公钥证书 PKC是一种包含持证主体标识、持证主体公钥等信息，并由可信签证机构（CA）签署的信息集合。
- 公钥证书主要用于确保公钥的安全，确保公钥与用户标识符之间绑定关系的安全。这个公钥就是证书所标识的那个主体的合法的公钥。
- 公钥证书的持证主体可以是人、设备、组织机构或其它主体。
- 公钥证书可以明文的形式进行存储和分配。

四、公钥证书的概念

- 任何一个用户只要知道签证机构的公钥，就能检查对证书签名的合法性。如果检查正确，那么用户就可以相信那个证书所携带的公钥是真实的，而且这个公钥就是证书所标识的那个主体的合法的公钥。
- 日常生活中有许多使用证书的例子，例如汽车驾照。驾照由可信的公安机关签发，以标识驾驶员的驾驶资格。由于有公安机关的签章，任何人都可以验证驾照的真实性。又由于驾照上印有驾驶员的照片并盖了钢印，从而实现驾驶员与驾照之间的严格绑定。

四、公钥证书的概念



简单公钥证书示意图

四、公钥证书的概念

- 有了公钥证书系统后，如果某个用户需要任何其他已向CA注册的用户的公钥，可向持证人（或证书机构）直接索取公钥证书。
- 用CA的公钥验证CA的签名，从而获得对公钥的信任。
- 由于公钥证书不需要保密，可以在网络上分发，从而实现公钥的安全网络分配。
- 又由于公钥证书有CA的签名，攻击者不能伪造合法的公钥证书。因此，只要CA是可信的，公钥证书就是可信的，其公钥就是可信的。

四、公钥证书的概念

- 使用公钥证书的主要好处：

①用户只要获得用户的证书，就可以获得用户的公钥。

②用户只要获得CA的公钥，就可验证证书的真伪，从而安全地获得用户的公钥。

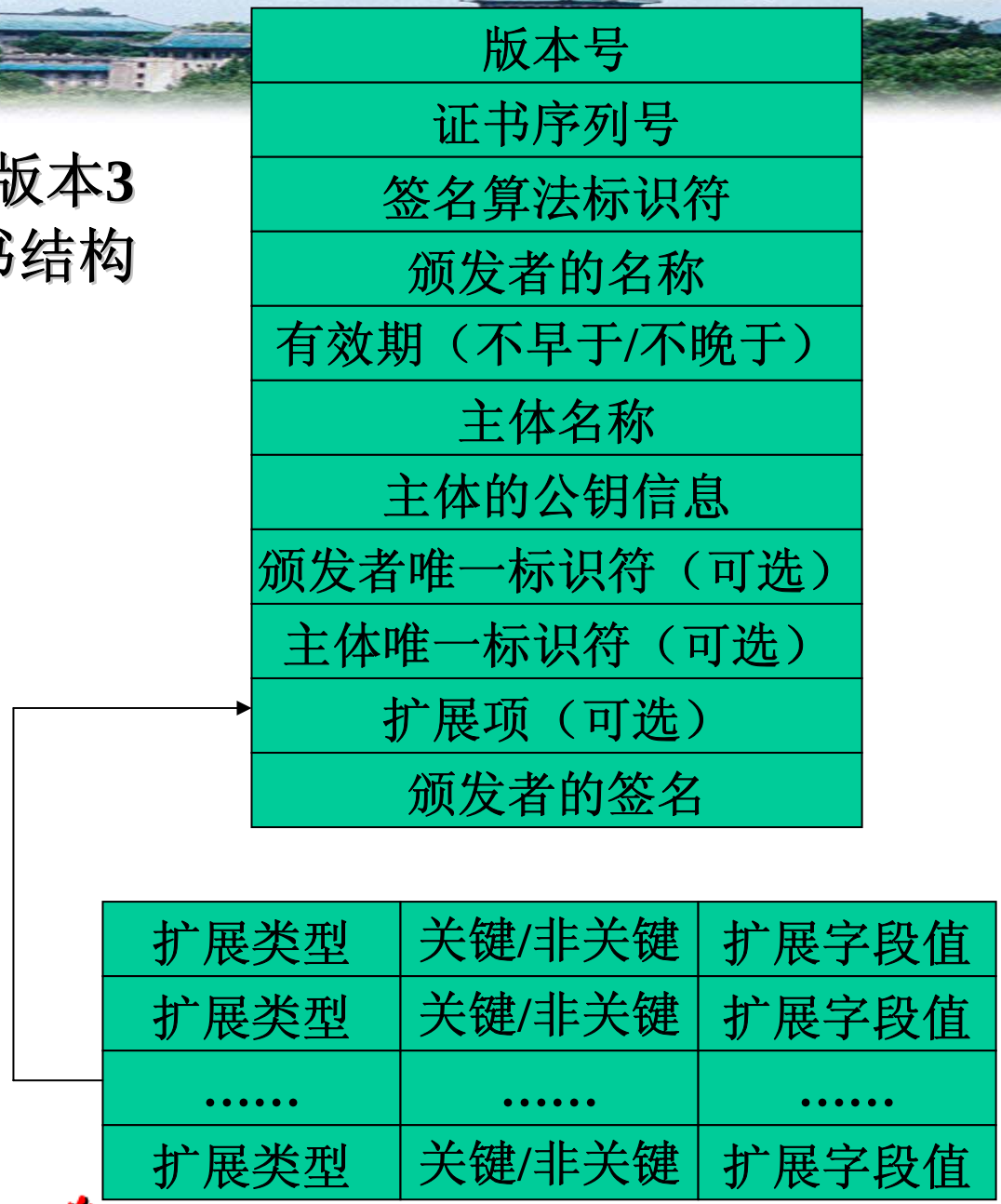
③因此公钥证书为公钥的分发奠定了基础，成为公钥密码在大型网络系统中应用的关键技术。

这就是电子政务、电子商务等大型网络应用系统都采用公钥证书的原因。

四、公钥证书的概念

- X.509证书
  - 目前应用最广泛的证书格式是国际电信联盟ITU（International Telecommunication Union）提出的X.509版本3格式。
  - X.509标准最早于1988年颁布。在此之后又于1993年和1995年进行过两次修改。
  - INTERNET工程任务组（IETF）针对X.509在INTERNET环境的应用，颁布了一个作为X.509子集的RFC2459。从而使X.509在INTERNET环境中得到广泛应用。

X.509版本3的证书结构



五、公钥基础设施PKI

- 公钥证书、证书管理机构、证书管理系统、围绕证书服务的各种软硬件设备以及相应的法律基础共同组成公开密钥基础设施**PKI**（**Public Key Infrastructure**）。

- 公开密钥基础设施提供一系列支持公开密钥密码应用（加密与解密、签名与验证签名）的基础服务。
- 本质上，**PKI**是一种标准的公钥密码的密钥管理平台。

五、公钥基础设施PKI

- 公钥证书是PKI中最基础的组成部分。
- 此外，PKI还包括签发证书的机构（CA），注册登记证书的机构（RA），存储和发布证书的目录，密钥管理，时间戳服务，管理证书的各种软件和硬件设备，证书管理与应用的各种政策和法律，以及证书的使用者。所有这些共同构成了PKI。

五、公钥基础设施PKI

1、签证机构CA

- 在PKI中，CA负责签发证书、管理和撤销证书。CA严格遵循证书策略机构所制定的策略签发证书。CA是所有注册用户所信赖的权威机构。

- CA在给用户签发证书时要加上自己的签名，以确保证书信息的真实性。为了方便用户对证书的验证，CA也给自己签发证书。这样，整个公钥的分配都通过证书形式进行。

五、公钥基础设施PKI

1、签证机构CA

- 对于大范围的应用，一个CA是远远不够的，往往要许多CA。
- 例如对于某一行业，国家建立一个最高级的CA，为根CA。
- 每个省建立一个省CA，每个地市也都可以建立CA，甚至一个企业也可以建立自己的CA。
- 不同的CA服务于不同的范围，履行不同的职责。

五、公钥基础设施PKI

2、注册机构RA

- RA（Registration Authority）是专门负责受理用户申请证书的机构。根据分工，RA并不签发证书，是负责对证书申请人的合法性进行认证，并决定是批准或拒绝证书申请。
- 接收证书申请人的注册信息，并对其合法性进行认证；
- 批准或拒绝证书的申请；
- 批准或拒绝恢复密钥的申请；
- 批准或拒绝撤销证书的申请；

五、公钥基础设施PKI

2、注册机构RA

- 对于一个小范围的系统，由CA兼管RA的职能是可以的。但随着用户的增多，CA与RA应当职责分开。
- 申请注册有不同的方式，有在线的方式和离线的方式。在INTERNET环境中可以WEB浏览器方式进行在线注册。注册的过程是用户与CA建立信任关系的一个重要步骤。

五、公钥基础设施PKI

3、证书的签发

- 经过RA的注册批准后，便可向CA申请签发证书。与注册方式一样，向CA申请签发证书可以在线申请，也可以离线申请。特别是在INTERNET环境中可以WEB浏览器方式在线申请签发证书，越来越受到欢迎。

五、公钥基础设施PKI

3、证书的签发

CA签发证书的过程如下：

- 用户向CA提交RA的注册批准信息及自己的身份等信息（或由RA向CA提交）；
- CA验证所提交信息的正确性和真实性；
- CA为用户产生密钥（或由用户自己产生并提供密钥），并进行备份；
- CA生成证书，并施加签名；
- 将证书存档入库，并将证书的一个副本交给用户。

五、公钥基础设施PKI

4、证书目录

- 证书产生之后，必须以一定的方式存储和发布，以便于使用。
- 为了方便证书的查询和使用，CA采用证书目录的式集中存储和管理证书。通常采用建立目录服务器证书库的方式为用户提供证书服务。
- 为了应用的方便，证书目录不仅存储管理用户的证书，还同时存储用户的相关信息（如，电子邮件地址，电话号码等）。因为证书本身是非保密的，因此证书目录也是非保密的。

五、公钥基础设施PKI

4、证书目录

- 证书目录提供了一种方便的证书存储和分发。
- 关于证书目录，目前尚没有一个统一的标准，但是基于X.500标准的目录正日益受到欢迎。
- 用于INTERNET环境的目录存取协议，并称为轻型目录存取协议LDAP（Lightweight Directory Access Protocol）。LDAP协议在目录模型上与X.500兼容，但比X.500更简单，实施更方便。

五、公钥基础设施PKI

5、证书的认证

证书认证主要包括以下内容：

① 验证证书上的CA签名是否正确。

② 验证证书内容的真实性和完整性。

③ 验证证书是否处在有效期内（由证书里的时间参数来限定有效期）。

④ 验证证书是否被撤销或冻结；

⑤ 验证证书的使用方式是否与证书策略和使用限制相一致。

五、公钥基础设施PKI

6、证书的撤销

- 每个证书都有一个有效使用期限，有效使用期限的长短由CA的政策决定。有效使用期限到期的证书应当撤销。
- 证书的公钥所对应的私钥泄露，或证书的持证人死亡，证书的持证人严重违反证书管理的规章制度等情况下也要撤销证书。
- 和证书的签发一样，证书的撤销也是一个复杂的过程。证书的撤销要经过申请、批准、撤销三个过程。

五、公钥基础设施PKI

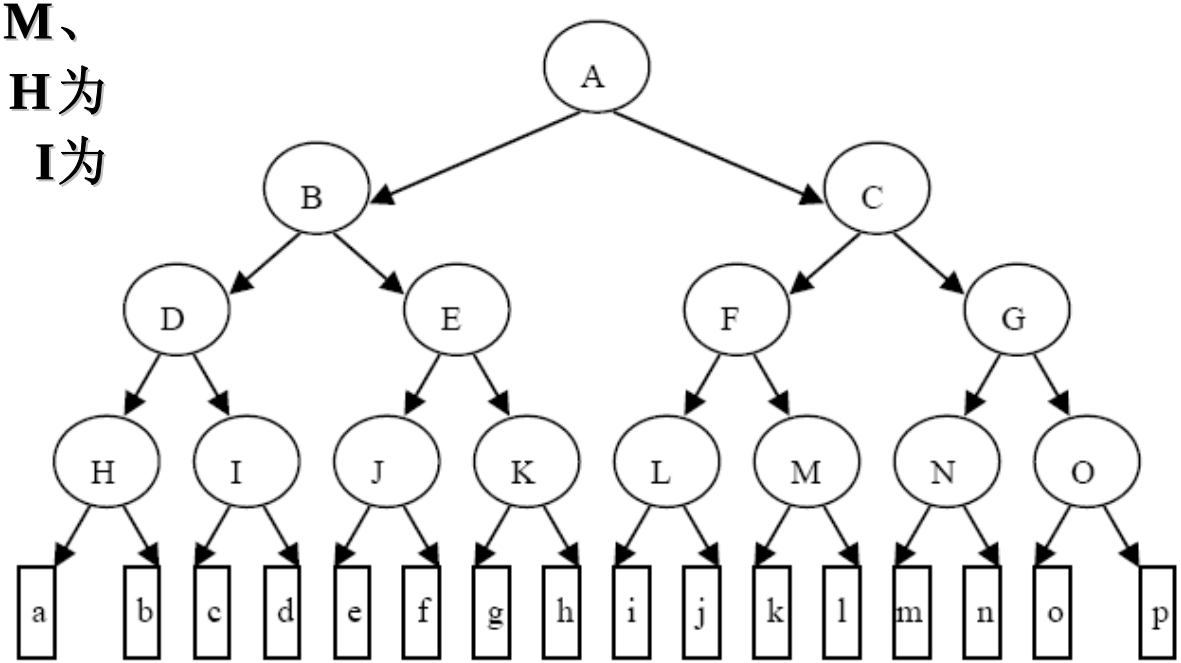
7、信任模型

- 对于大范围的PKI（如一个行业或一个地区，甚至一个国家。），一个CA也是不现实的，往往需要多CA。
- 这些CA之间应当具有某种结构关系，以使不同CA之间的证书认证简单方便。
- 证书用户、证书主体、各个CA之间的证书认证关称为PKI的信任模型。
- 人们已经提出了树（层次）模型、森林模型等多种信任模型。

五、公钥基础设施PKI

7、信任模型

- 树模型
  - 大写字母表示CA，小写字母表示用户，箭头表示证书的签发关系。
  - A是根CA。B和C是二级CA。D、E、F、G是三级CA。H、I、J、K、L、M、N、O是四级CA。H为用户a和b签发证书，I为用户c和d签发证书。



五、公钥基础设施PKI

7、信任模型

- 在树型模型中，一个证书持证者至少必须知道两个CA的公钥，一个是直接为其签发证书的CA，另一个是根CA。
- 设a要与p进行保密通信，于是a要获得p的公钥，为此a要获得p的证书。假设a通过目录服务获得了p的证书，但是p的证书是由O签名的，必须用O的公钥才能认证，而a只有H的公钥。为了获得O的公钥，必须获得O的证书，但为了认证O证书又必须获得G的公钥。为了获得G的公钥，必须获得G证书，但为了认证G的证书又必须获得C的公钥。为了获得C的公钥，必须获得C的证书，但为了认证C的证书又必须获得A的公钥。而A是根CA。因此所有其他CA和最终用户都知道A的公钥。

五、公钥基础设施PKI

7、信任模型

- 于是，a只要知道A的公钥，依次获得并验证C的证书、G的证书、O的证书和p的证书，便可以获得p的公钥，并且可以相信p的公钥。于是a便可以与p进行保密通信。
- 可见，用户a为了获得p的公钥，依次验证了A给C签发的证书，C给G签发的证书，G给O签发的证书，O给p签发的证书，共经历四个证书的验证。形象地把A→C→G→O→p称为对p的证书的验证路径，路径长度为4。
- 一般，一个*n*层树结构模型，任何两个用户之间都有一条唯一的验证路径，而且路径的长度为*n*。

谢　谢！