§6.1 密钥管理策略

- 所有的密码技术都依赖于密钥
- 密钥的管理本身是一个很复杂的课题而且是保证安全性的关键点
- 密钥管理方法因所使用的密码体制（对称密码体制和公钥密码体制）而异，通常要借助于加密、认证、签名等技术，
- 密钥管理系统中常常依靠可信赖第三方参与的公证系统。公证系统可以协助实现密钥的分配和证实，而且可以作为证书机构、时戳代理、密钥托管代理和公证代理等。

§6.1 密钥管理策略

密钥类型：

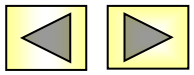
1、基本密钥（Base Key)

2、会话密钥（Session Key）

3、密钥加密密钥（Key Encrypting Key）

4、主机主密钥（Host Master Key）

5、在公钥体制下的还有公开密钥、私有密钥、签名密钥之分。



§6.1 密钥管理策略

密钥类型：

1、基本密钥（Base Key)

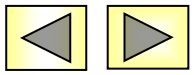
又称初始密钥（Primary Key) 或用户密钥(User key)，是由用户选定或由系统分配给用户的，可在较长时间（相对于会话密钥）内由一对用户所专用的密钥。

2、会话密钥（Session Key）

3、密钥加密密钥（Key Encrypting Key）

4、主机主密钥（Host Master Key）

5、在公钥体制下的还有公开密钥、私有密钥、签名密钥之分。



§6.1 密钥管理策略

密钥类型：

1、基本密钥（Base Key)

2、会话密钥（Session Key）

即两个通信终端用户在一次通话或交换数据时使用的密钥，当它用于加密文件时，称为文件密钥(File key)，当它用于加密数据时，称为数据加密密钥(Data Encrypting Key)

3、密钥加密密钥（Key Encrypting Key）

4、主机主密钥（Host Master Key）

5、在公钥体制下的还有公开密钥、私有密钥、签名密钥之分。

§6.1 密钥管理策略

密钥类型：

1、基本密钥（Base Key)

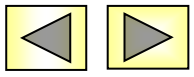
2、会话密钥（Session Key）

3、密钥加密密钥（Key Encrypting Key）

用于对会话密钥或文件密钥进行加密时采用的密钥。又称辅助二级密钥或密钥传送密钥。通信网中的每个节点都分配有一个这类密钥。

4、主机主密钥（Host Master Key）

5、在公钥体制下的还有公开密钥、私有密钥、签名密钥之分。



§6.1 密钥管理策略

密钥类型：

1、基本密钥（Base Key)

2、会话密钥（Session Key）

3、密钥加密密钥（Key Encrypting Key）

4、主机主密钥（Host Master Key）

对密钥加密密钥进行加密的密钥，存于主机处理器中。

5、在公钥体制下的还有公开密钥、私有密钥、签名密钥之分。

§6.1 密钥管理策略

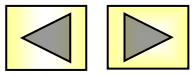
密钥生存期：

- 所有的密钥都有生存期（有效期）
- 密钥的生存周期：授权使用该密钥的周期
- 原因：
  - 使用时间越长，泄露机会越大，破译的诱惑越大。
  - 密钥泄露时间越长，损失越大。
  - 同一密钥加密，密码分析更容易。
- 主密钥生存期长；会话密钥生存期短；加密保存数据文件的密钥不能经常变换（每个文件用一个密钥加密，所有密钥用密钥加密密钥加密）；用作数字签名和身份鉴别的私有密钥生存期长。

§6.1 密钥管理策略

- 一个密钥主要经历以下几个阶段：
  - 产生（可能需要登记）
  - 分配
  - 使用
  - 更新/替换
  - 撤销
  - 销毁





§6.1 密钥管理策略

密钥管理：

- 在一种安全策略指导下密钥的产生，存储，分配，删除，归档及应用
- 处理密钥自产生到最终销毁的整个过程中的有关问题，包括系统的初始化，密钥的产生、存储、备份/恢复、装入、分配、保护、更新、控制、丢失、吊销和销毁等内容。
- 分配和存储是其中最棘手的问题。
- 密钥管理的目的：维持系统中各实体之间的密钥关系以抗击各种可能的威胁，如密钥的泄露、秘密密钥或公开密钥的身份的真实性丧失、经未授权使用

§6.1 密钥管理策略

密钥的产生：

- 手工/自动化
- 选择密钥方式不当会影响安全性，如：

(1)使密钥空间减小

	4字节	5字节	6字节	7字节	8字节
小写字母（26）	$4.6*10^5$	$1.2*10^7$	$3.1*10^8$	$8.0*10^9$	$2.1*10^{11}$
小写字母+数字（36）	$1.7*10^6$	$6.0*10^7$	$2.2*10^9$	$7.8*10^{10}$	$2.8*10^{12}$
字母数字字符（62）	$1.5*10^7$	$9.2*10^8$	$5.7*10^{10}$	$3.5*10^{12}$	$2.2*10^{12}$
印刷字符（95）	$8.1*10^7$	$7.7*10^9$	$7.4*10^{11}$	$7.0*10^{13}$	$6.6*10^{15}$
ASCII字符（128）	$2.7*10^8$	$3.4*10^{10}$	$4.4*10^{12}$	$5.6*10^{14}$	$7.2*10^{16}$
8位ASCII字符（256）	$4.3*10^9$	$1.1*10^{12}$	$2.8*10^{14}$	$7.2*10^{16}$	$1.8*10^{19}$

§6.1 密钥管理策略

(2)差的选择方式易受字典式攻击。

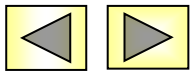
攻击者并不按照数字顺序去试所有可能的密钥，首先尝试可能的密钥，例如英文单词、名字等。(Daniel Klein使用此法可破译40%的计算机口令)

方法如下：

- 用户的姓名、首字母、帐户名等个人信息
- 从各种数据库得到的单词
- 数据库单词的置换
- 数据库单词的大写置换
- 对外国人从外国文字试起
- 尝试词组

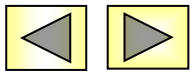
§6.1 密钥管理策略

- 好的密钥具有如下特点：
  - 真正随机、等概，如掷硬币。
  - 避免使用特定算法的弱密钥。
  - 双钥系统的密钥必须满足一定的数学关系。
  - 选择长度适中，易记且难猜中的密钥。
  - 适当采用杂凑技术，将易记的长密钥经单向杂凑函数变换成伪随机数串。



§6.1 密钥管理策略

- 不同等级的密钥的产生方式不同
  - 主机主密钥安全性至关重要，故要保证其完全随机性、不可重复性和不可预测性。可用投硬币、掷骰子、噪声发生器等方法产生
  - 密钥加密密钥数量大(N(N-1)/2)，可由机器自动产生，安全算法、伪随机数发生器等产生
  - 会话密钥可利用密钥加密密钥及某种算法(加密算法，单向函数等)产生
  - 初始密钥类似于主密钥或密钥加密密钥的方法产生



§6.1 密钥管理策略

- 必须在安全环境中产生密钥以防止对密钥的非授权访问
- 密钥产生形式有两种：
  - 由中心(或分中心)集中生产，如传统的密钥分发中心KDC 和证书分发中心CDC等方案，其密钥的认证协议简洁，交易中的安全责任由中心承担
  - 由个人分散生产，密钥变量中的公钥必须公开需经第三方认证，交易中安全责任由个人承担
- 密钥登记

将产生的密钥与特定的使用捆绑在一起。例如用于数字签名的密钥必须与签名者的身份捆绑在一起，这个捆绑必须通过某一授权机构来完成

§6.1 密钥管理策略

密钥的保护：

- 密钥的安全保密是密码系统安全的重要保证。除了公钥密码系统中的公钥外，所有的密钥需要保密
- 所有密钥的完整性也需要保护，因为一个入侵者可能修改或替代密钥，从而危及机密性服务
- 在实际中最安全的方法是将其放在物理上安全的地方
- 当密钥无法用物理的办法安全保护时，必须用其它的方法
  - 将一个密钥分成两部分委托给两个不同的人
  - 通过机密性(如用另一个密钥加密)或完整性服务来保护
- 极少数密钥(主机主密钥)以明文存储于有严密物理保护的密码器中，其他密钥都被(主密钥或次主密钥)加密后存储

§6.1 密钥管理策略

密钥的存储：

- 密钥存储时必须保证密钥的机密性、认证性和完整性，防止泄漏和修正。
- 方法：
  - 将所有密钥或公钥存储在专用媒体(软盘、芯片等) 一次性发放给各用户，用户在本机中就可获得对方的公钥，协议非常简单，又很安全。电脑黑客的入侵破坏，也只能破坏本机，而不影响其他终端。这种形式只有在**KDC**等集中式方式下才能实现。
  - 用对方的公钥建立密钥环各自分散保存，如**PGP**
  - 将各用户的公钥存放在公用媒体中。

§6.1 密钥管理策略

密钥的备份：

- 为防止保管密钥的人出现意外，密钥必须有备份，以恢复用其加密的信息。
- 密钥备份方法：
  - 使用秘密共享协议
  - 使用智能卡暂存

§6.1 密钥管理策略

密钥的销毁（吊销）：

- 清除一个密钥的所有踪迹。
- 在密钥的使用活动终结后，安全地销毁所有敏感密钥的拷贝是十分重要的。因为攻击者可用它来读取曾经用它加密的文件，且旧密钥有利于分析密码体制。
- 密钥的安全是协议、算法和密码技术设备安全的基本。一旦密钥泄漏，安全保密性就无从谈起。唯一的办法就是更换密钥。若密钥由**KDC**管理，则用户需及时通知**KDC**将其销毁；若无**KDC**，则应及时告诉可能和他通信的人，且加上时戳。
- 在特定的环境中密钥的销毁是必须的。

§6.1 密钥管理策略

密钥的使用控制：

- 对密钥的使用进行限制，保证密钥按预定的方式使用。
- 控制信息：
  - 密钥的主权人
  - 密钥的合法使用期限
  - 密钥的识别符
  - 密钥的用途
  - 限定的算法
  - 预定使用的系统或环境或密钥的授权用户
  - 与密钥生成、注册、证书有关的实体名称
  - 密钥的完整性校验

