密 码 学

（第十五讲）

密钥管理

张焕国

武汉大学计算机学院

目　录

1、密码学的基本概念
2、古典密码
3、数据加密标准（DES）
4、高级数据加密标准（AES）
5、中国商用密码（SMS4）
6、分组密码的应用技术
7、序列密码
8、习题课：复习对称密码
9、公开密钥密码（1）

目　录

10、公开密钥密码（2）
11、数字签名（1）
12、数字签名（2）
13、HASH函数
14、认证
15、*密钥管理*
16、PKI技术
17、习题课：复习公钥密码
18、总复习/检查：*综合实验*

一、密钥管理的概念

- 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，从密钥管理的途径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。*

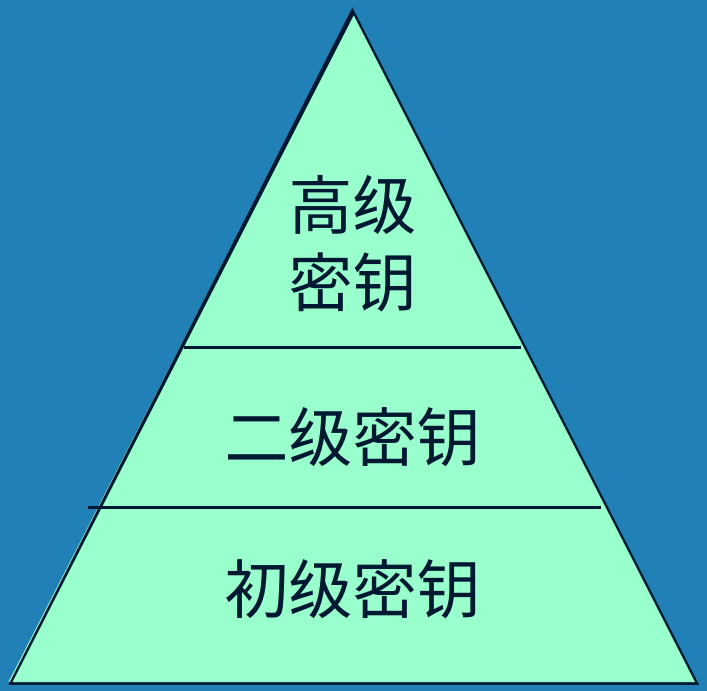
二、密钥管理的原则

- 区分密钥管理的策略和机制。
- 全程安全原则。
- 最小权利原则。
- 责任分离原则。
- 密钥分级原则。
- 密钥更换原则。
- 密钥应当安全：长度足够，随机等。
- 密码体制不同，密钥管理也不相同。

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。
- 其中用于通信保密的初级密钥为初级通信密钥，并记为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。*

三、传统密码的密钥管理

①初级密钥

- 初级文件密钥与其所保护的文件有一样长的生存周期。
- 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

- 二级密钥可经专职密钥安装人员批准，由系统自动产生。
- 可由专职密钥安装人员提供。
- 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。
- 二级密钥必须接受更高级的密钥的保护。

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随机产生，并妥善安装。
- 主密钥的生存周期很长。

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随机性：长周期性、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再现的。任何人都不能再次产生它。*
- *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
- 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，可借助于主密钥和一个强的密码算法来产生二级密钥。*

三、传统密码的密钥管理

2、密钥产生

- 用产生主密钥的方法产生两个真随机数RN_1，RN_2，再产生一个随机数RN_3，然后分别以它们为密钥对一个序数进行四层加密，最后产生出二级密钥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*初密钥的产生*

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

$RD=E(K_s, K_M)$或 $RD=E(K_f, K_M)$，

$RD=E(K_s, K_{NC})$或 $RD=E(K_f, K_{NF})$。

三、传统密码的密钥管理

2、*密钥产生*

③*初密钥的产生*

- ***使用初级密钥时，用高级密钥将随机数RN解密：***

  $K_s = \mathbf{D}(RD, K_M)$或 $K_f = \mathbf{D}(RD, K_M)$，

  $K_s = \mathbf{D}(RD, K_{NC})$或 $K_f = \mathbf{D}(RD, K_{NF})$

- ***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*

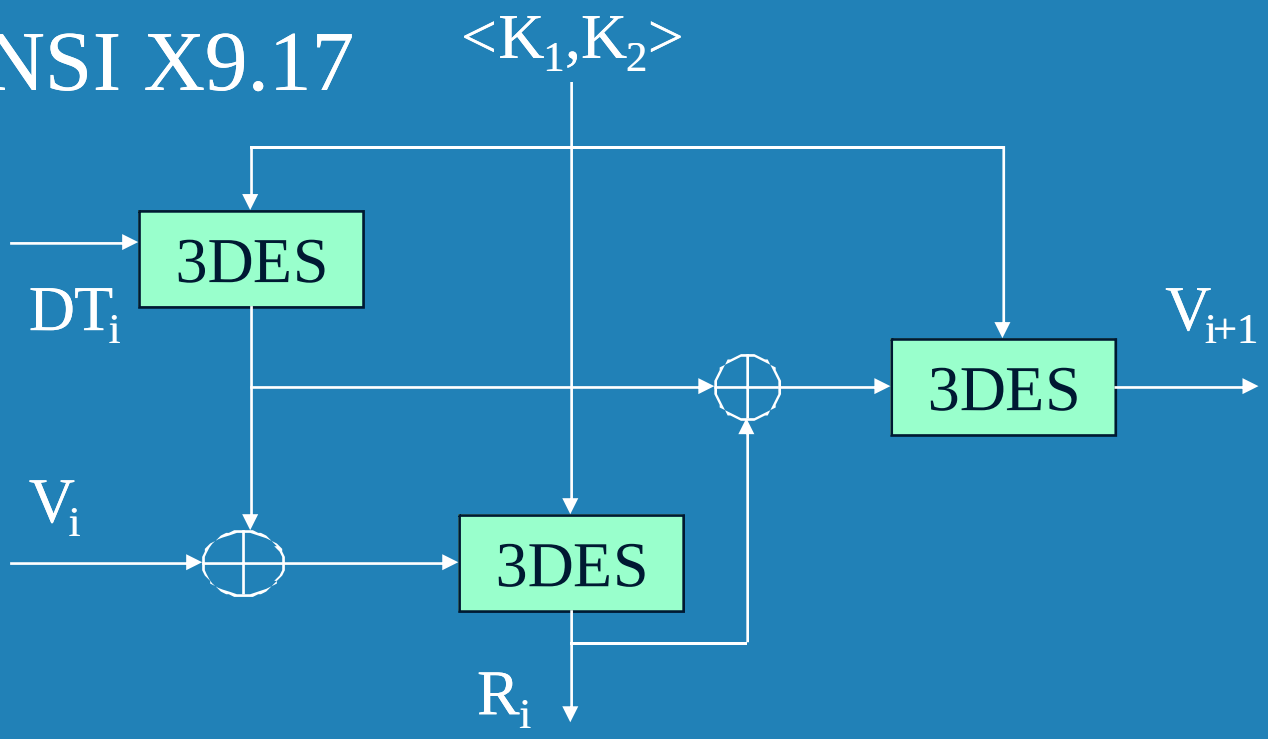
④*伪随机数的产生*

- *二级密钥和初级密钥的产生都需要伪随机数。*
- *伪随机性：长周期，均匀分布，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

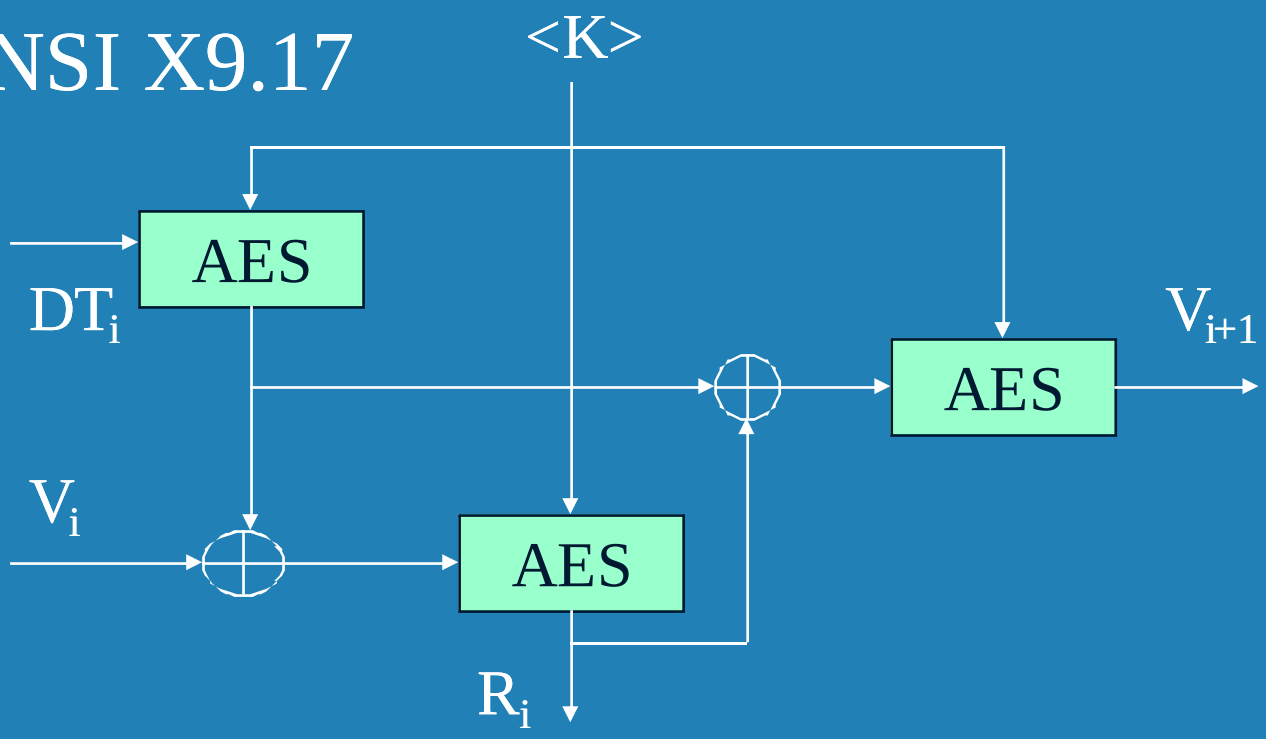


- ***美国电子支付标准，因特网的PGP采用***

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。

三、传统密码的密钥管理

2、*密钥分配*

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

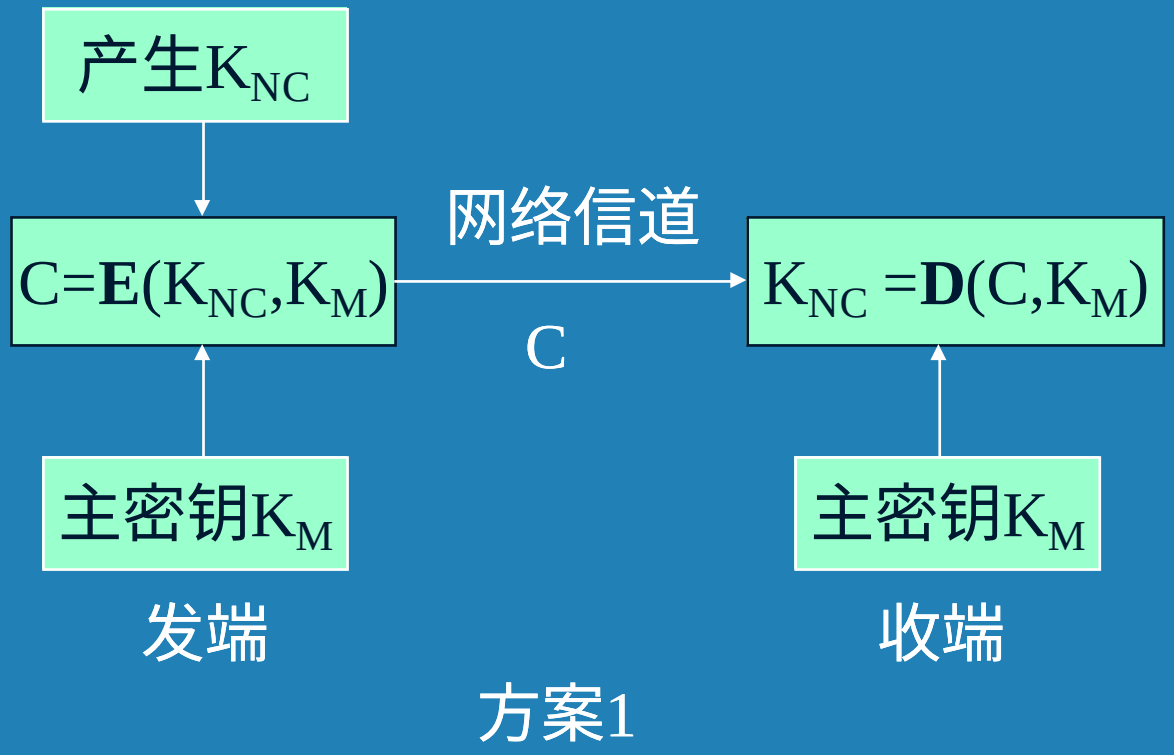
2、*密钥分配*

②二级密钥的分配

- *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。*
- *另一种方法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

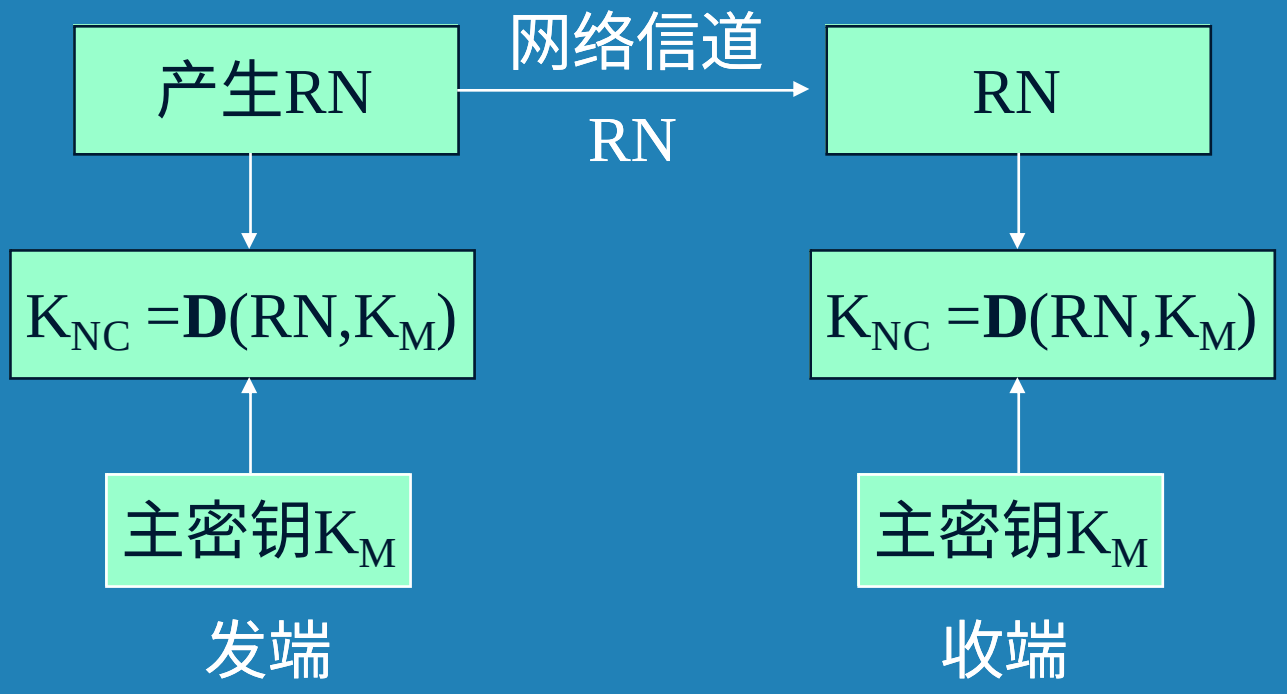
2、*密钥分配*



方案1

三、传统密码的密钥管理

2、*密钥分配*



方案2

三、传统密码的密钥管理

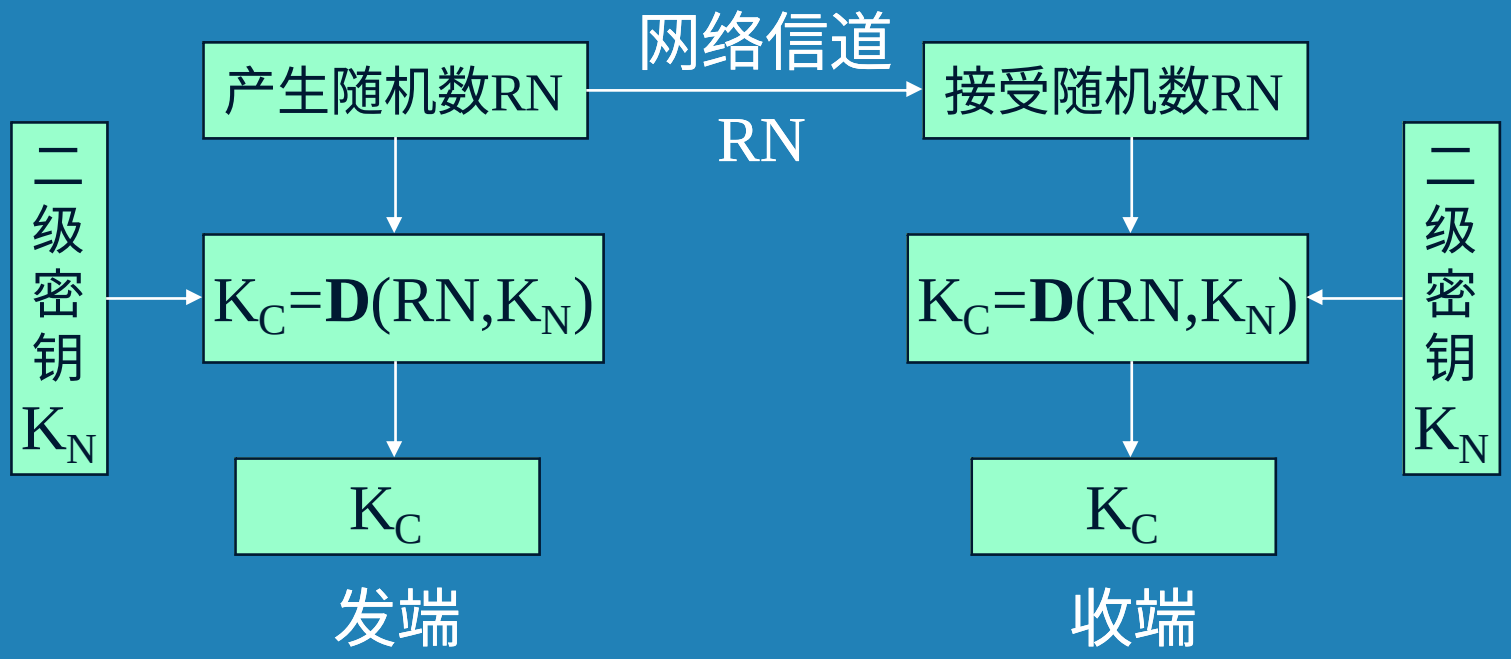
2、*密钥分配*

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*



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。*
- *要求存储器必须是高度安全的，物理上是安全的，而且逻辑上也是安全的。*
- *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*

- *二级密钥可以以明文形态存储，也可以以密文形态存储。*
- *如果以明文形态存储，则要求存储器必须是高度安全的。*
- *如果以密文形态存储，则对存储器的要求可适当降低。*
- *通常采用以高级密钥加密的形式存储二级密钥。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。*

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。*


谢 谢！