# 密 码 学

## 第十六讲　密钥管理（1）

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室

# 内容简介

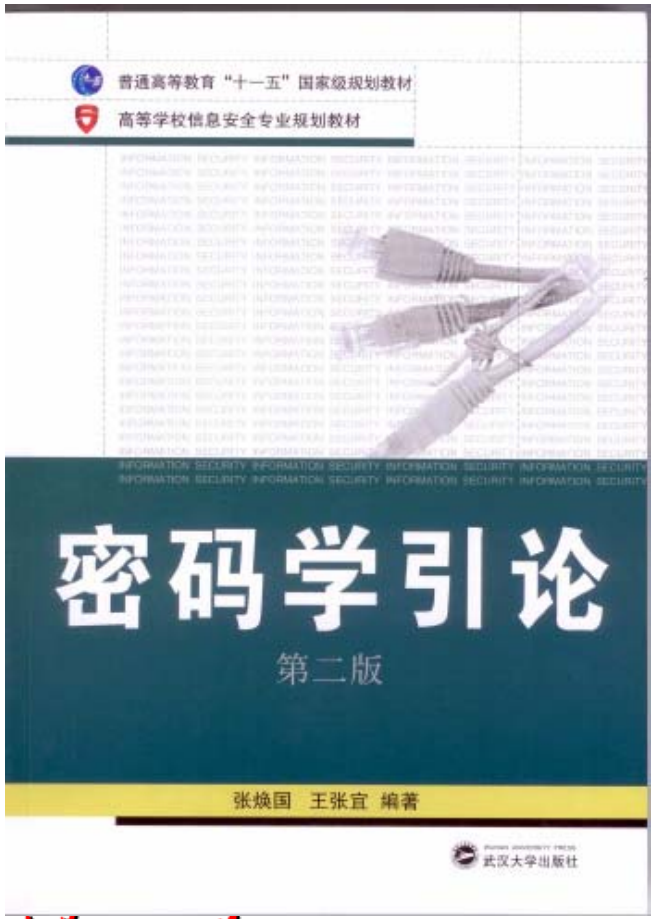
第一讲 信息安全概论
第二讲 密码学的基本概念
第三讲 数据加密标准（DES）
第四讲 高级数据加密标准（AES）
第五讲 中国商用密码（SMS4）
第六讲 分组密码的应用技术
第七讲 序列密码
第八讲 复习
第九讲 公钥密码（1）

# 内容简介

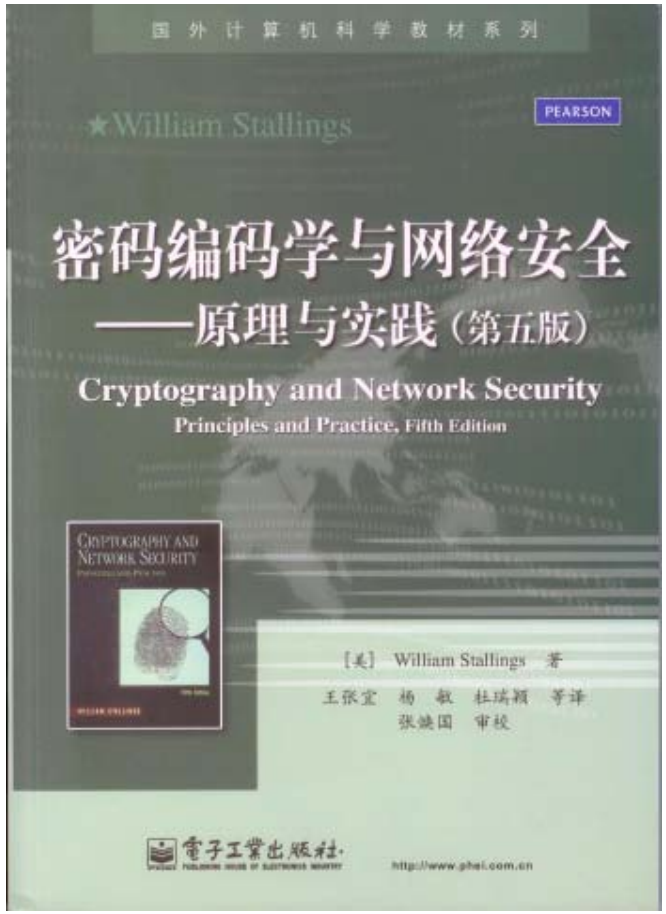
第十讲 公钥密码（2）
第十一讲 数字签名（1）
第十二讲 数字签名（2）
第十三讲 HASH函数
第十四讲 认证
第十五讲 密码协议
第十六讲 密钥管理（1）
第十七讲 密钥管理（2）
第十八讲 复习

# 教材与主要参考书

教材




参考书



# 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。

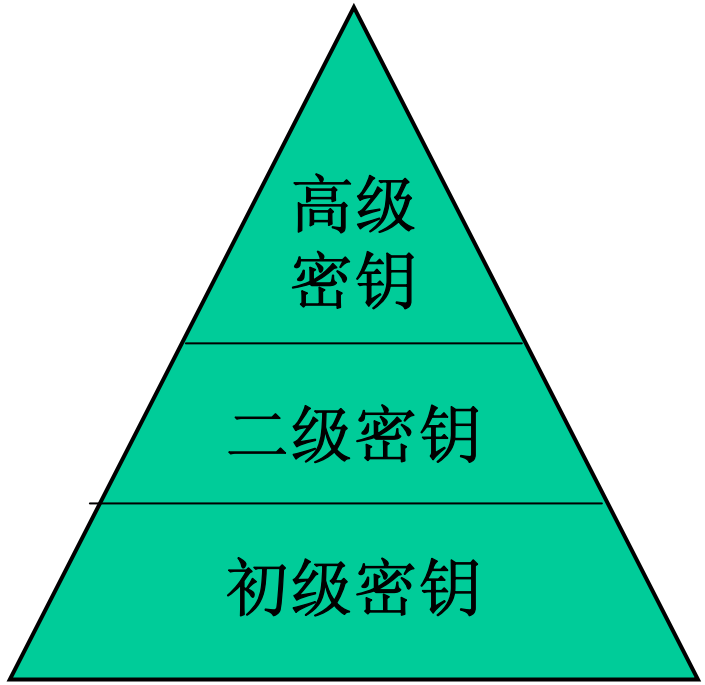
# 二、密钥管理的原则

- 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。

# 二、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 )



# 二、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$K_f$ 。

# 二、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。

# 二、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$K_{NF}$。

# 二、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。

# 二、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！

# 二、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。

# 二、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。

# 二、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。
- 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。

# 二、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：

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

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

- 好处：安全，一产生就是密文，方便。

# 二、传统密码的密钥管理

## 2、密钥产生

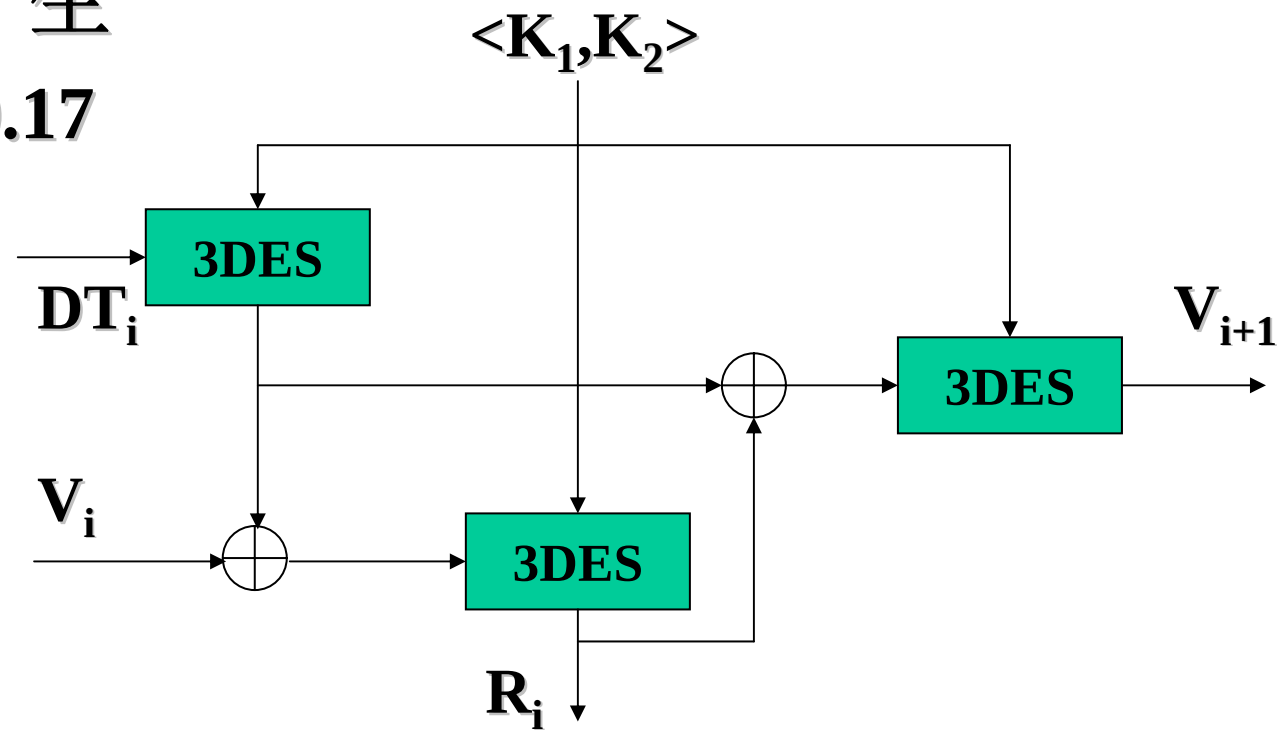
④伪随机数的产生

- 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

# 二、传统密码的密钥管理

## 2、密钥产生

- ANSI X9.17

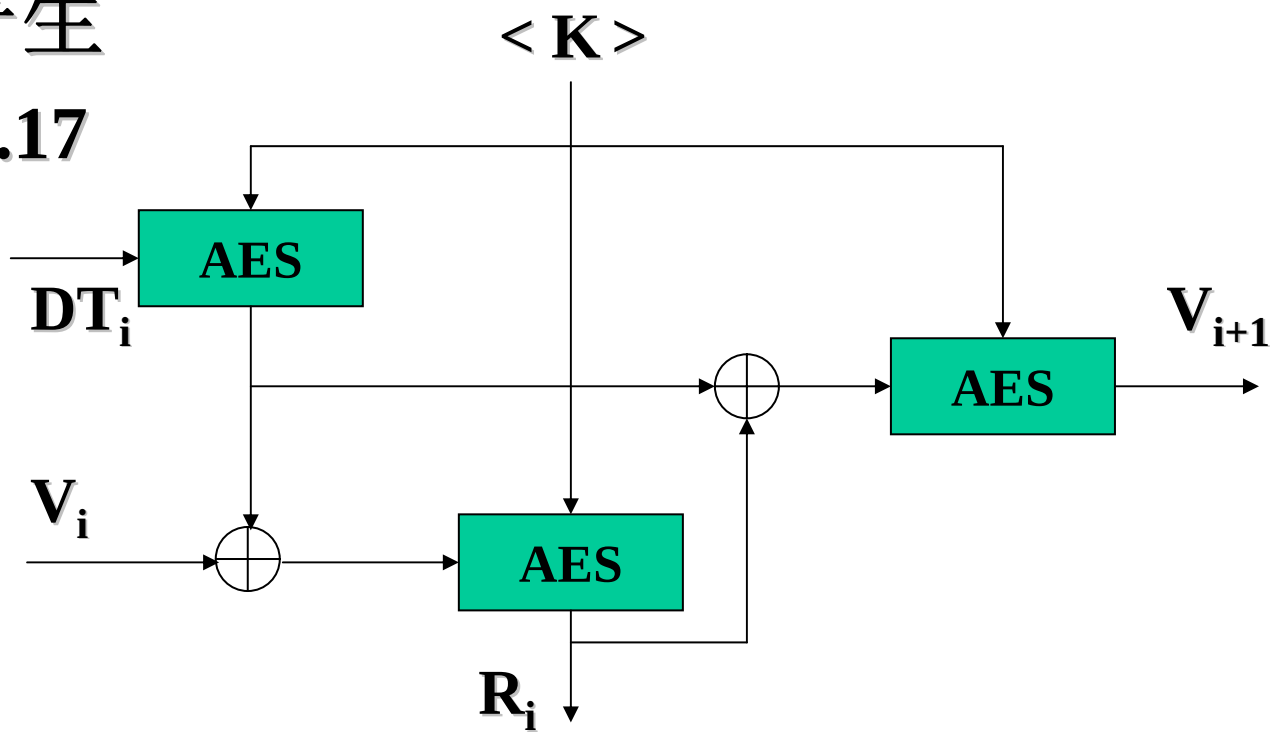



- 美国电子支付标准，因特网的PGP采用

# 二、传统密码的密钥管理

## 2、密钥产生

- ANSI X9.17




AES方案

# 二、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。

# 二、传统密码的密钥管理

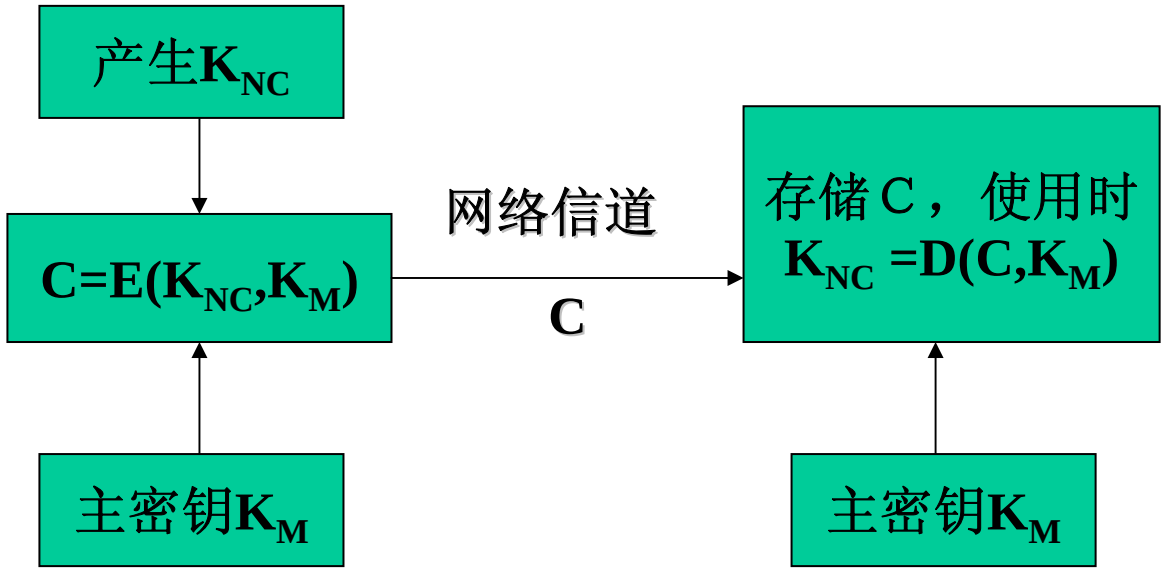
## 2、密钥分配

### 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。

# 二、传统密码的密钥管理

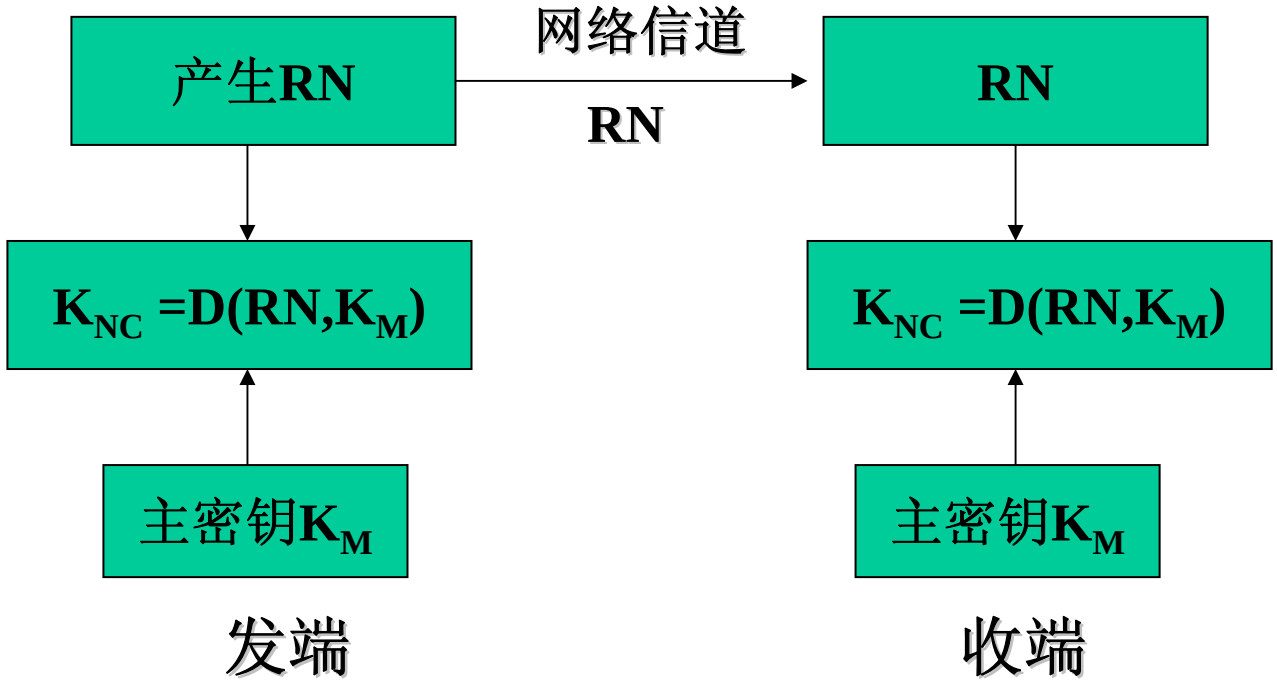
## 2、密钥分配




方案1原理图

# 二、传统密码的密钥管理

## 2、密钥分配




方案2原理图

# 二、传统密码的密钥管理

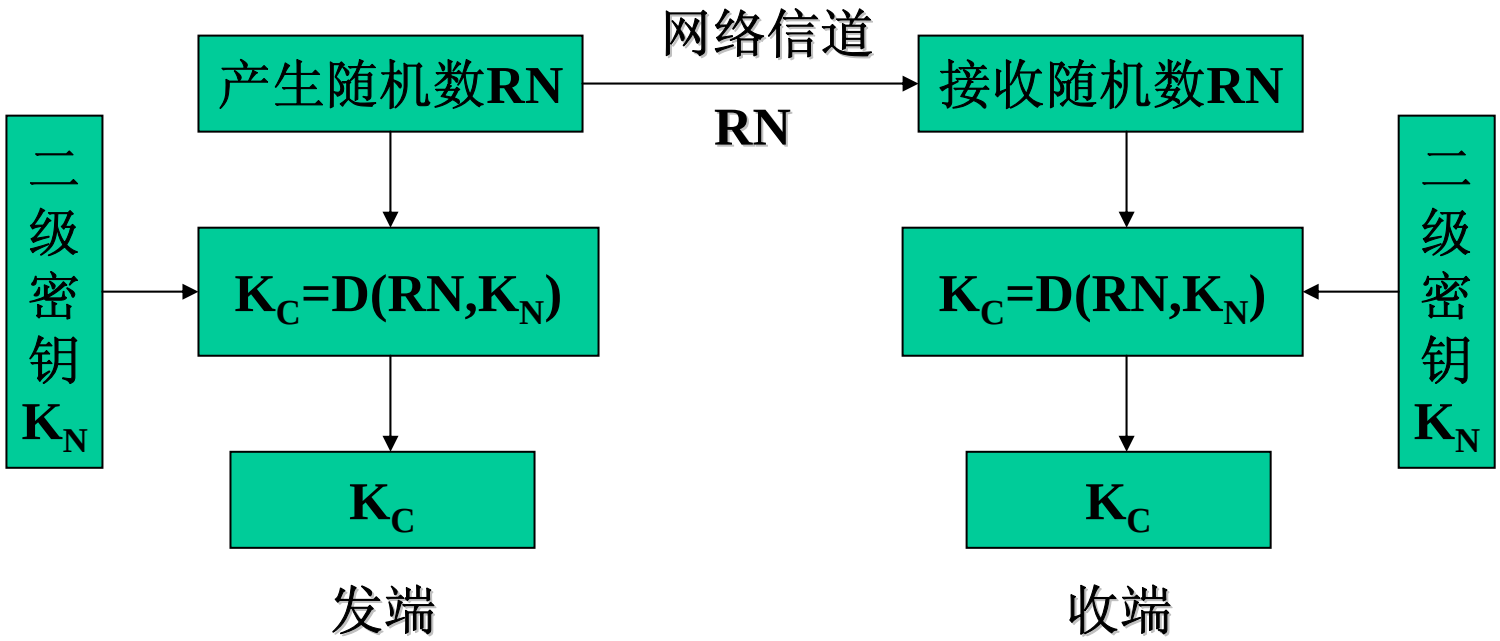
## 2、密钥分配

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。

# 二、传统密码的密钥管理

## 2、密钥分配




原理图



武漢大学

# 二、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。

# 二、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。

# 二、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。

# 二、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。

# 二、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。

# 二、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。

# 二、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。

# 二、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。

# 作 业 题

**1、p279第6题。**

# 谢　谢！