第五讲 保密通信

郑燕飞

保密通信

- 面临的攻击
  - 局域网内监听
  - 搭线窃听
- 传输媒介
  - 线缆(双绞线、同轴电缆、光纤)
  - 微波链路
  - 卫星信道
- 等等、等等

链路加密与端到端加密

- 链路加密
  - 每个通信链路两端都装备加密设备
  - 要求许多加密设备
  - 报文在传输中多次加解密
  - 报文在每个交换机处以明文形式存在
  - 用户对报文的安全无法控制
  - 能够鉴别主机

链路加密与端到端加密

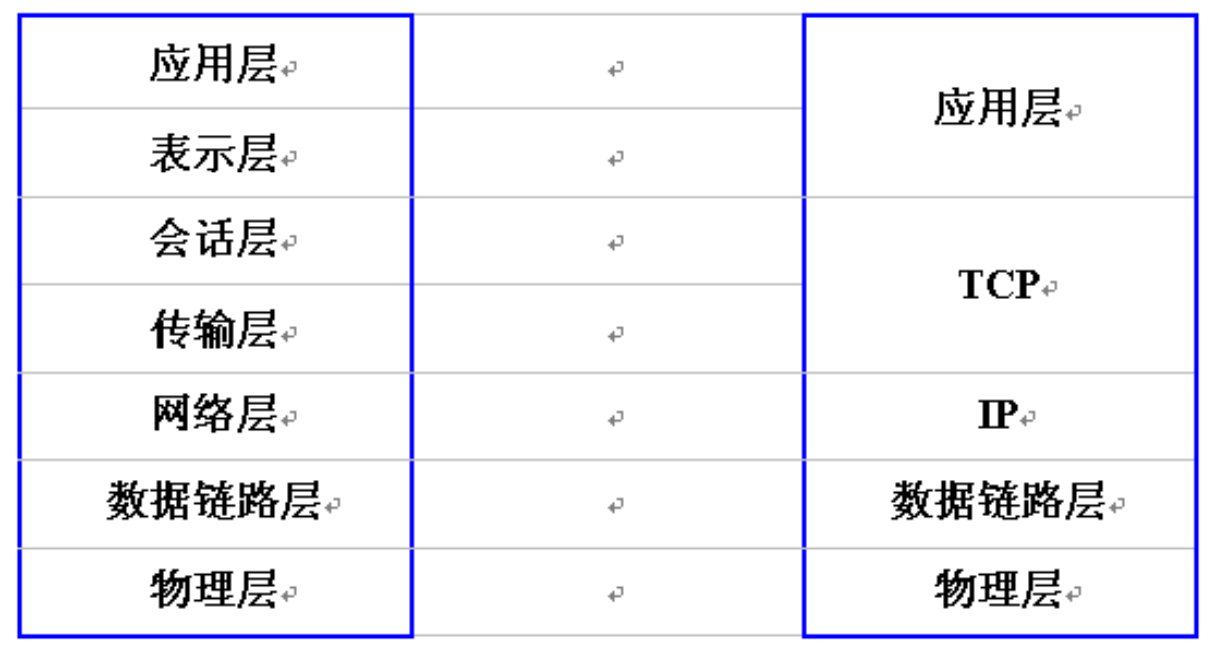
- 端到端加密
  - 加密过程由两个端系统完成
  - 报文在传输中只进行一次加解密
  - 报文在交换机处仍然是安全的
  - 不能隐蔽通信量
  - 能够鉴别用户

两种方式的比较

链路加密	端到端加密
在发送主机上报文是暴露的	在发送主机上报文是暴露的
在中间结点上报文是暴露的	在中间结点上报文是加密的
由发送主机应用	由发送进程应用
对用户是透明的	用户应用加密
主机维护加密设施	用户决定算法
所有用户用同一个设施	用户选择加密方案
可以由硬件完成	软件实现
所有或没有报文被加密	用户选择是否对每个报文加密
主机和中间结点、中间结点之间共享密钥	每对用户之间共享密钥
提供主机鉴别	提供用户鉴别

* 两种方式共用

网络体系结构模型

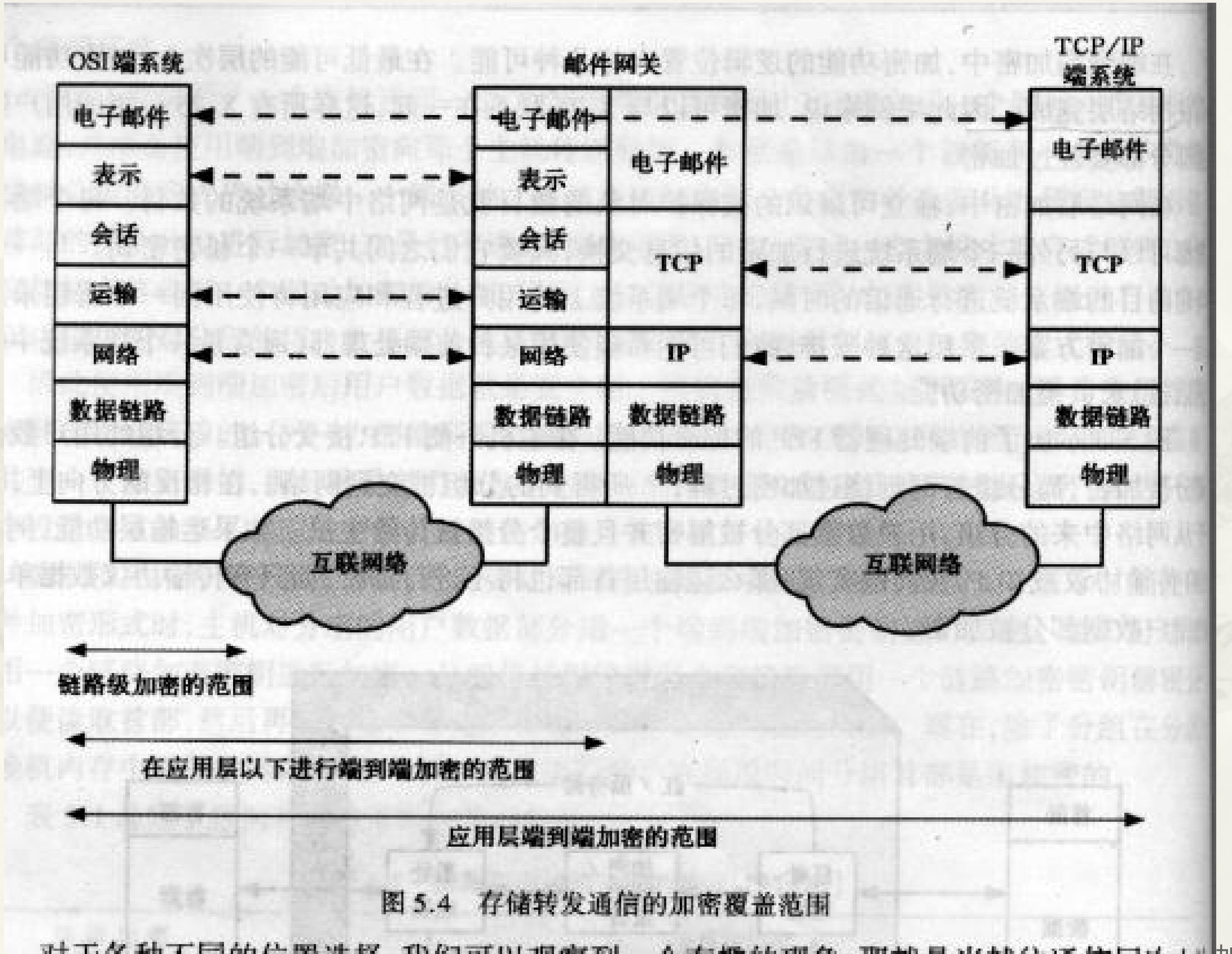


OSI模型　　实际常用

加密的逻辑位置

- 链路加密处于物理层或者链路层
- 端到端加密
  - 网络层
  - 应用层
    - 两个不同体系结构的网络之间
    - 相同体系结构但相互隔离的网络之间
- 前端处理器

加密覆盖范围图



OSI端系统
邮件网关
TCP/IP
端系统
电子邮件
表示
会话
运输
网络
数据链路
物理
TCP
IP
互联网络
链路级加密的范围
在应用层以下进行端到端加密的范围
应用层端到端加密的范围
图 5.4 存储转发通信的加密覆盖范围

通信量的机密性

- 可从通信量中得到的信息
  - 通信双方的身份
  - 通信双方通信的频率
  - 报文模式、报文长度、报文数量
  - 特定的通信之间交谈所关联的事件
  - 隐信道
    - 以一种通信设施设计者未设想的方式进行通信的方法
    - 例如：报文的长度

通信量的机密性

- 防范手段
  - 链路加密方式
    - 分组首部加密
    - 通信量填充
  - 端到端加密方式
    - 填充数据单元
    - 发送空白报文

密钥分配

- 密钥分配方式
  - 由A选定，物理地传送给B
  - 第三方选定，物理地传送给A和B
  - 使用A和B共有的密钥加密后传送给另一方
  - A和B都有到第三方的加密连接，则由第三方用加密连接传送给A和B
- 分析
  - 1，2需人工传递，对于链路加密时合理的
    对于端到端加密，密钥分配难度比较大
  - 3 一旦暴露一个密钥，后续密钥都暴露了
  - 4适合于端到端加密，有许多变体

一个简单的密钥分配方案

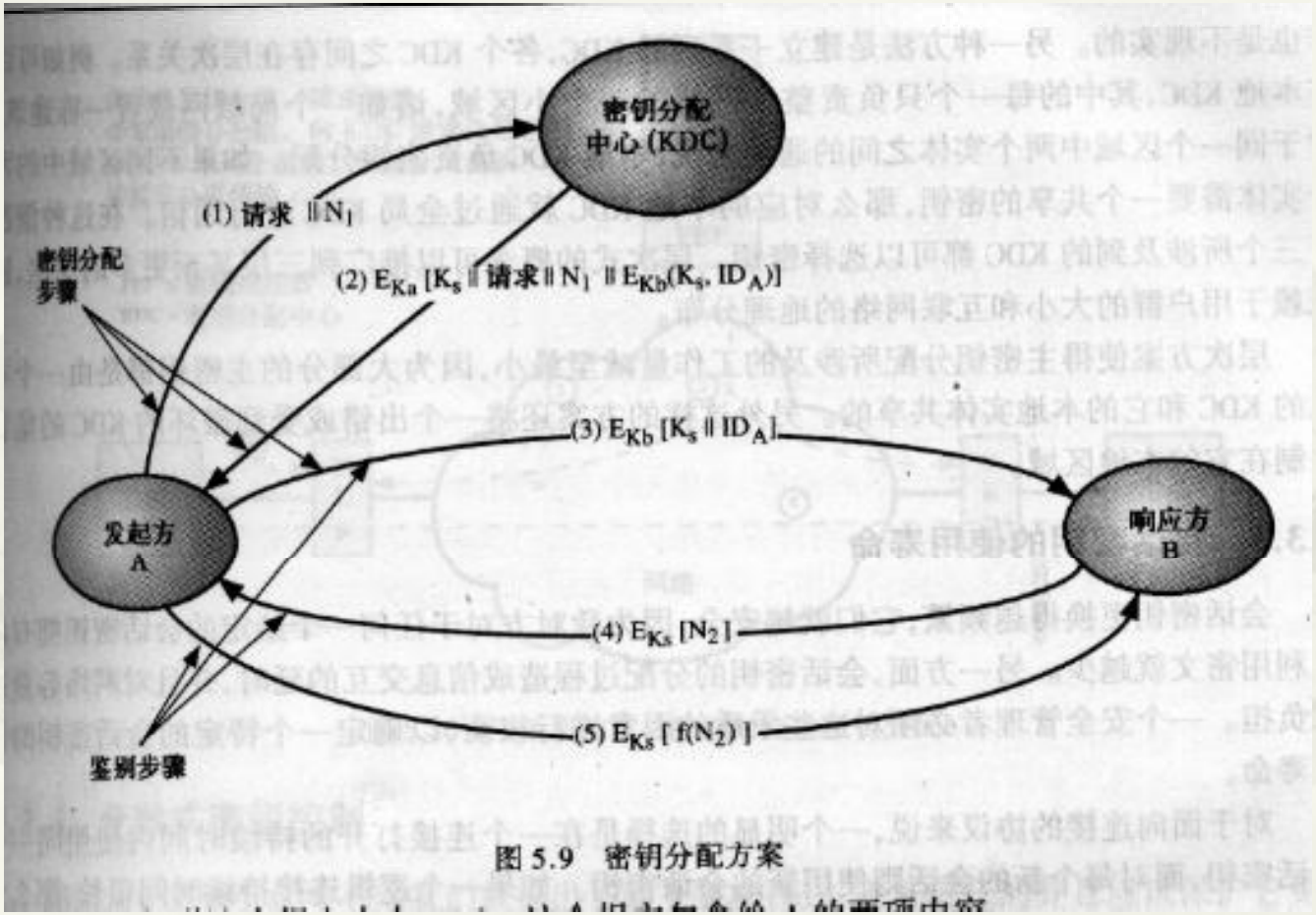


图 5.9 密钥分配方案

- KDC，Ka，Kb，Ks
- 现时（nonce）
  - 对于一次交互的唯一标志符
  - 时间戳、计数器、随机数
  - 以上的组合

层次式密钥分配方案

- 层次式
  - 建立一系列KDC，各个KDC之间存在层次关系
  - 最低层的负责某一区域
  - 不同区域之间的通信通过上一层KDC进行
- 优点
  - 主密钥的分配工作量减小
  - 整个系统鲁棒性强

透明的密钥控制方案

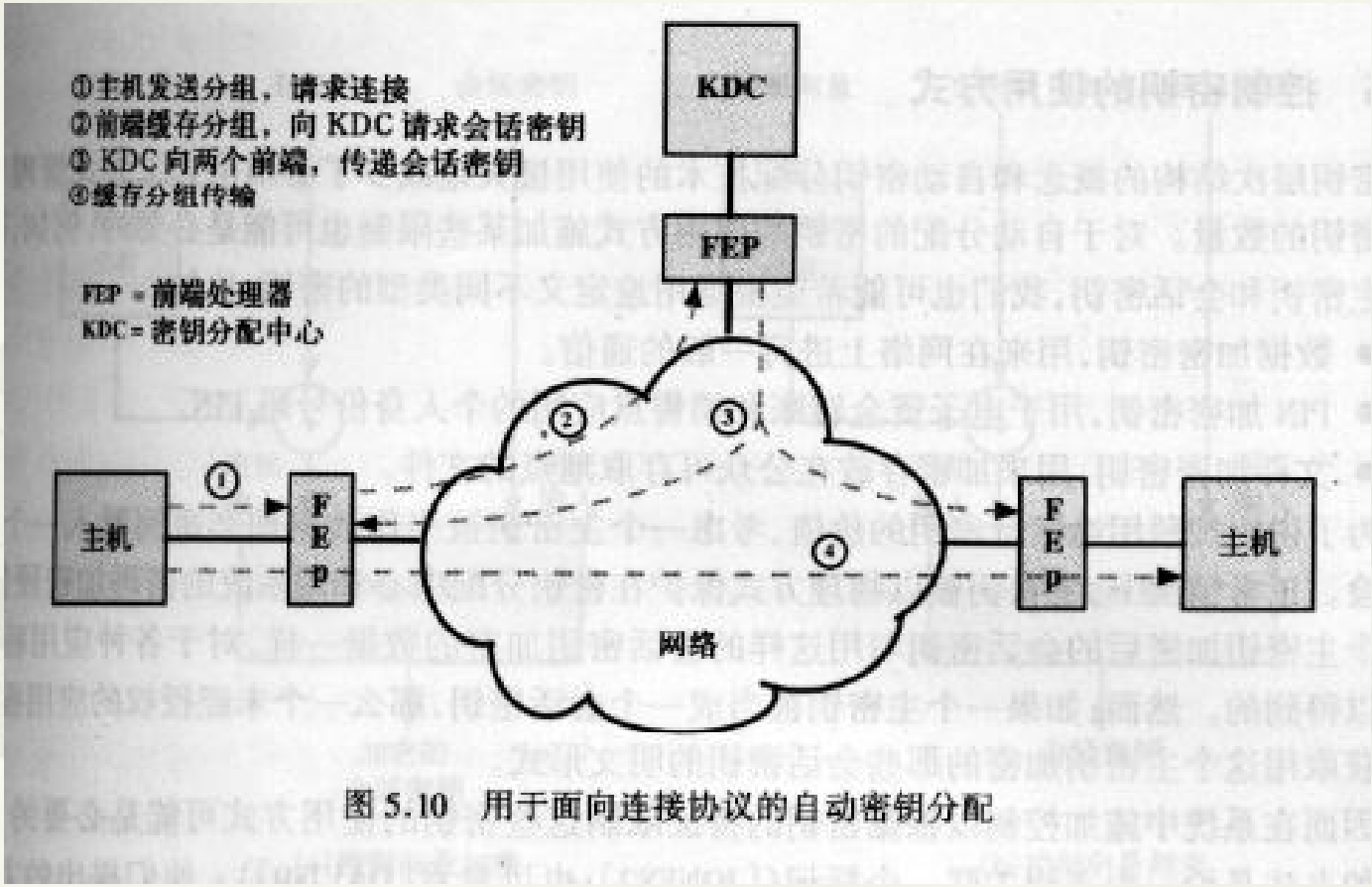


图 5.10　用于面向连接协议的自动密钥分配

分散式密钥控制

图 5.11　分散化的密钥分配

会话密钥的寿命

- 会话密钥的分配过程给网络会造成负担
- 对于面向连接的协议
  - 一个连接一个会话密钥
  - 如果连接时间很长，则可以选择PDU序号循环周期作为会话密钥的寿命长度
- 对于无连接的协议
  - 一个交互过程一个会话密钥
  - 固定时间段或者一定数量的交互量后更换一次会话密钥

控制密钥的使用方式

- 密钥的不同种类
  - 数据加密密钥
  - PIN加密密钥
  - 文件加密密钥
- 使用校验码的比特位
  - 一种基于DES的区分密钥的方式
  - 一个比特指示是会话密钥还是主密钥
  - 一个比特指示是否可用于加密
  - 一个比特指示是否可用于解密
  - 其他比特保留

使用控制向量

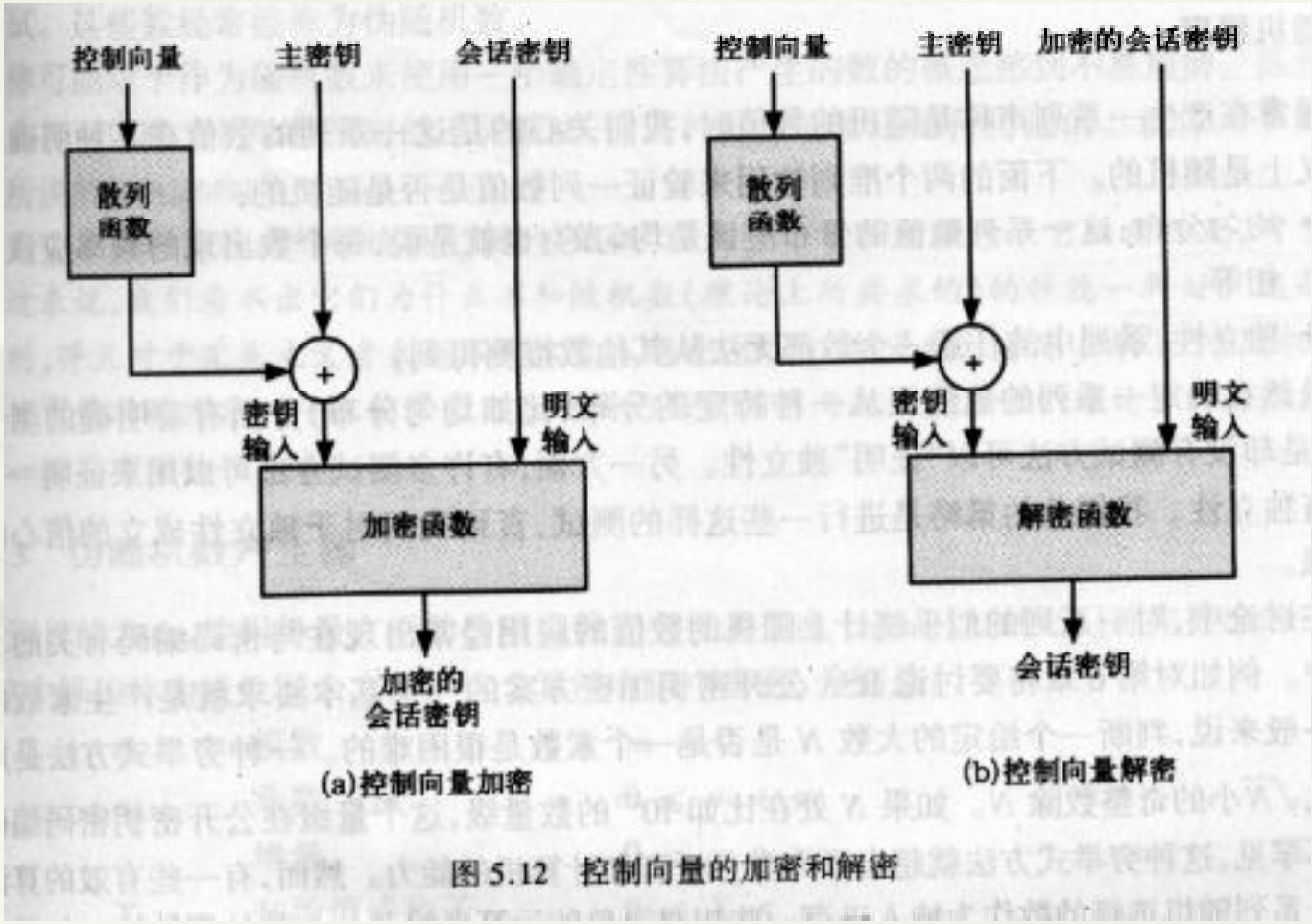


图 5.12 控制向量的加密和解密

随机数

- 随机数的用途
  - 鉴别方案(nonce)
  - 会话密钥的产生
  - RSA公开密钥加密算法中密钥的产生
- 检验随机程度的两个准则
  - 均匀分布
  - 独立性
- 不可预测程度

伪随机数产生器

- 线性同余法

$$X_{n+1} = (aX_n + c) \bmod m$$

  - m 模数 m>0
  - a 乘数 0<=a<m
  - c 增量 0<=c<m
  - X0 初始值 0<=X0<m
  - 一般将m选为一个给的计算机所能表示的最多非负整数
  - 此方法受到很彻底的测验
  - 一旦知道序列的一小部分，不可预测程度就变得很差

密码编码方式产生的随机数

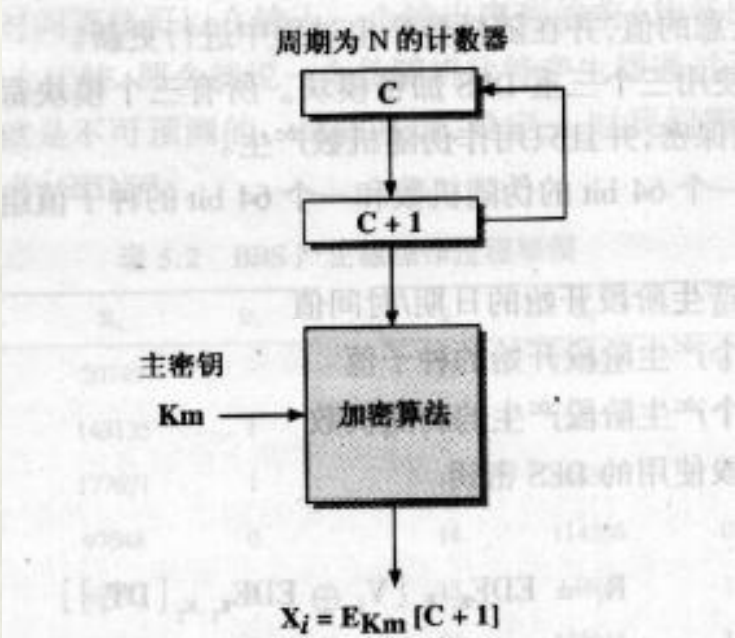


图 5.13　从一个计数器产生伪随机数

BBS产生器

- 选择两个大素数，满足
$$p \equiv q \equiv 3 (\mathrm{mod}\, 4)$$
- n=p*q,选择s与n互素
- 那么：
$$X_0 = s^2 \bmod n$$
$$X_i = (X_{i-1})^2 \bmod n$$
$$B_i = X_i \bmod 2$$

END