**古典密码🡪现代密码**

* **古典密码**
  + 对字符或单词进行处理 (加解密)
  + 明文一般是有意义的自然语言文本
* **现代密码**
  + 面向计算机和芯片（对比特、字节或字进行处理）
  + 明文可以是任意比特串

**密码体制安全性的两种定义（无条件安全性，计算安全性）**

1. **无条件安全性（信息论角度）**

即使攻击者拥有无限的计算资源，也无法被破译

1. **计算安全性（计算复杂性角度）**

攻击者用(现在或将来)可得到的资源无法破译

**讨论加密体制的安全性时，需要考虑两点：**

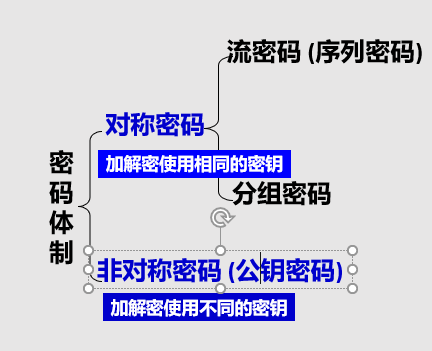
* 1. **能抵抗攻击者什么类型的攻击**

唯密文攻击、已知明文攻击……

* 1. **能阻止攻击者实现什么样的目标**

找到密钥、破译特定的密文……

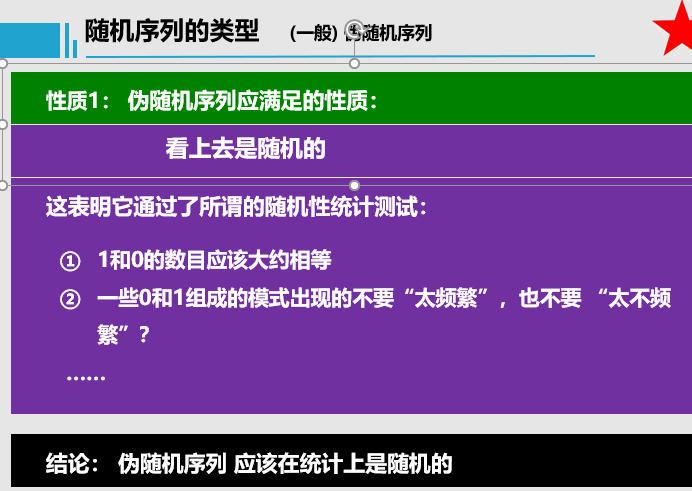
**攻击者的攻击能力越强，要实现的目标越低，越难对付**



**计算机本身只能产生伪随机序列**

**随机序列的类型**

**1. (一般) 伪随机序列**



**2. 密码学意义上安全的伪随机序列**

**性质2：并不是任何伪随机序列都能用于密码学， 密码学意义上安全的伪随机序列还必须具备另一个性质：不可预测性。**

**不可预测性即使知道了产生序列的算法、以前产生的所有比特，也不可能通过计算来预测下一个比特是什么（准确预测成功的概率很低）目的是防止攻击者在知道若干比特后，成功猜测后续比特**

**3. 真随机序列**

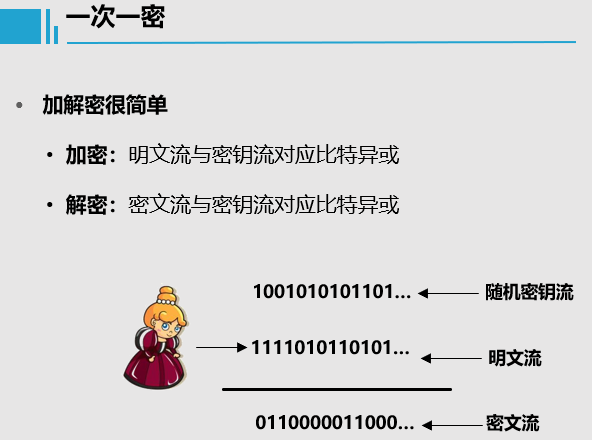
**不能被可靠地重复产生**

**用完全同样的输入操作两次，得到的是两个不相关的序列**

**Q: 如何得到真随机序列？**

**使用一种专门的设备(真随机数发生器)，输入是各种无法预测的信号：周围空气状况、电流的变化率…**

* **输入是不断变化的，输出也就不可重复。**
* **有人能预测产生的下一个数吗？ 他必须重构输入信号，这没人能做到**



一次一密

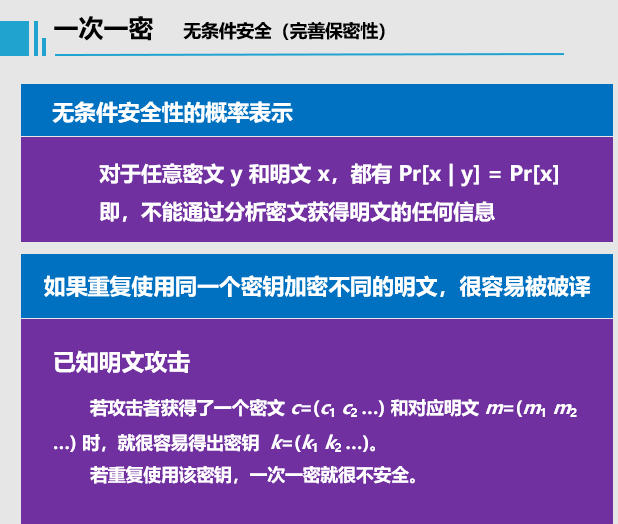
特点：**密钥流是真随机序列，且不重复使用(故得名 一次一密)**

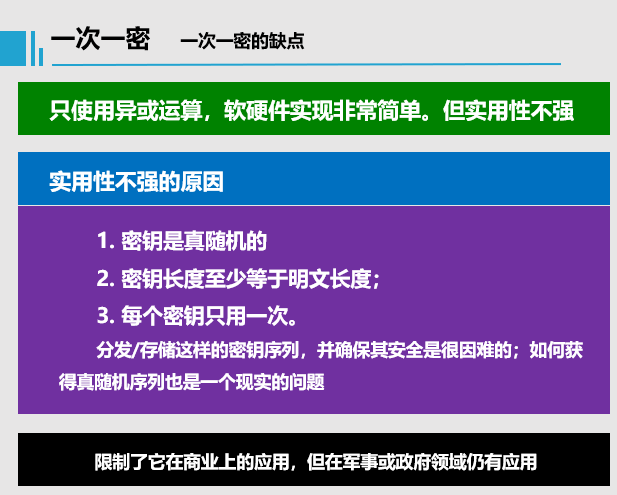
安全性：**因为密钥流是真随机的，所以没人能预测下一个比特**

**具有无条件安全性（完善保密性）：**

**即使攻击者具有无限的计算资源，也无法破译一次一密 (理论上不可破译，无条件安全的)**

**原因：密钥是随机的，而且明文与密钥是统计上相互独立的，使得密文也是随机的，故而密钥的随机性很好的隐藏了明文的统计特性**





一次一密的缺点（密钥是真随机，长度要等于明文长度，每个密钥只能用一次）

**流密码**

**流密码的基本思想：**

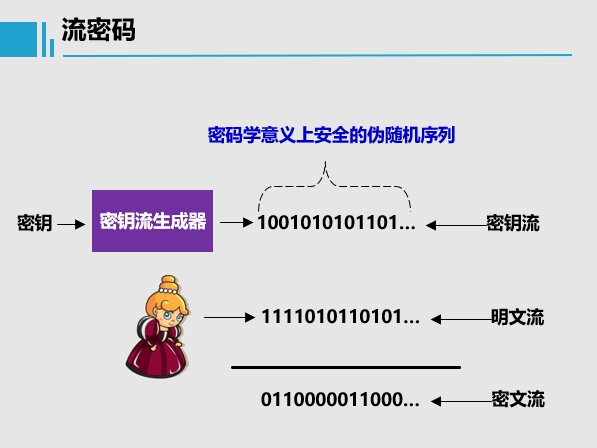
**用一个较短的密钥生成密钥流，在攻击者(计算能力是有限的)看来是随机的(伪随机的)。**

**不是无条件安全的，仅是计算上安全的**

**产生密钥流的任务由密钥流生成器完成：**

**输入：“较短的密钥”**

**输出： 源源不断的密钥流**



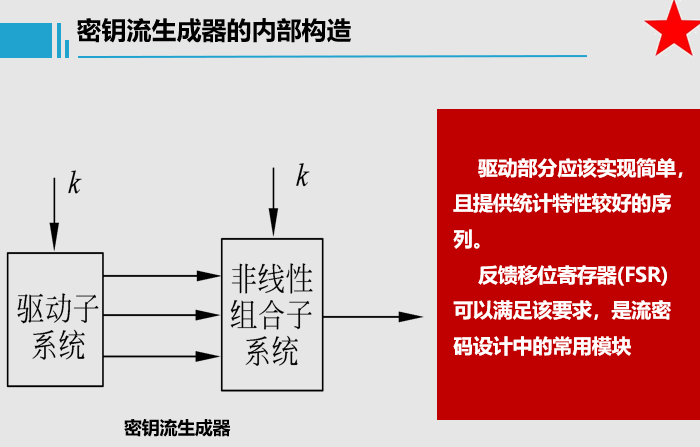
**密钥流生成器的组成（驱动部分和非线性组合部分）**

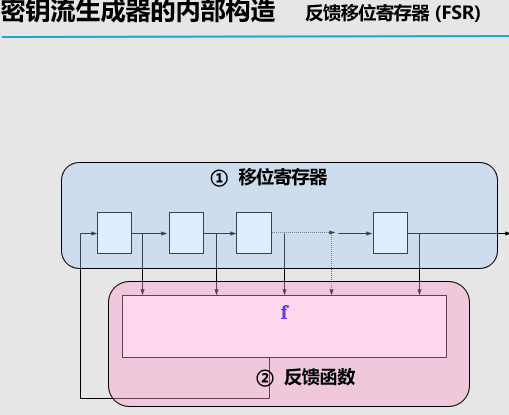
1.驱动部分

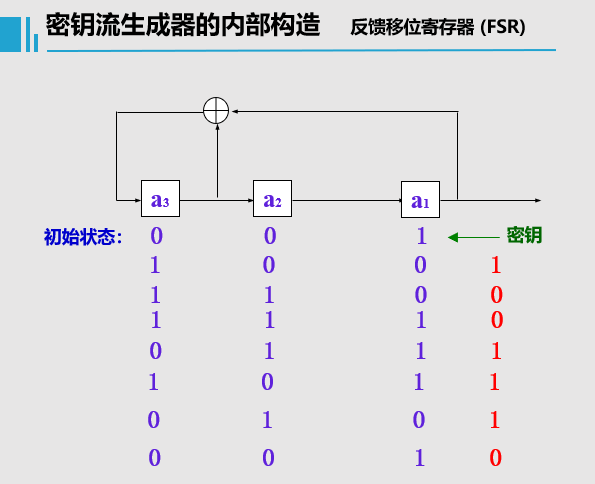
为非线性组合部分提供统计特性“好”的序列 (一般伪随机序列)

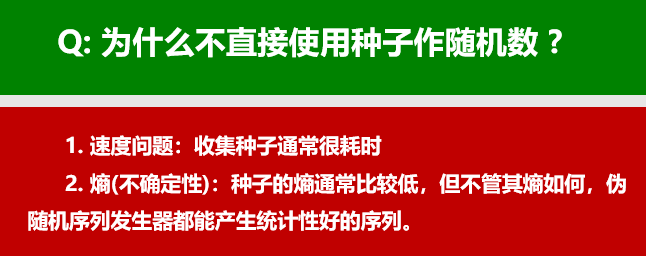
2.非线性组合部分

将提供的输入序列组合成密码学特性“好”的序列 (密码学意义上安全的伪随机序列)



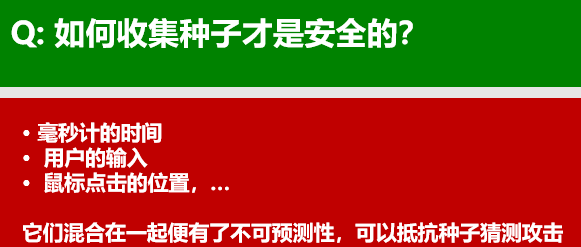


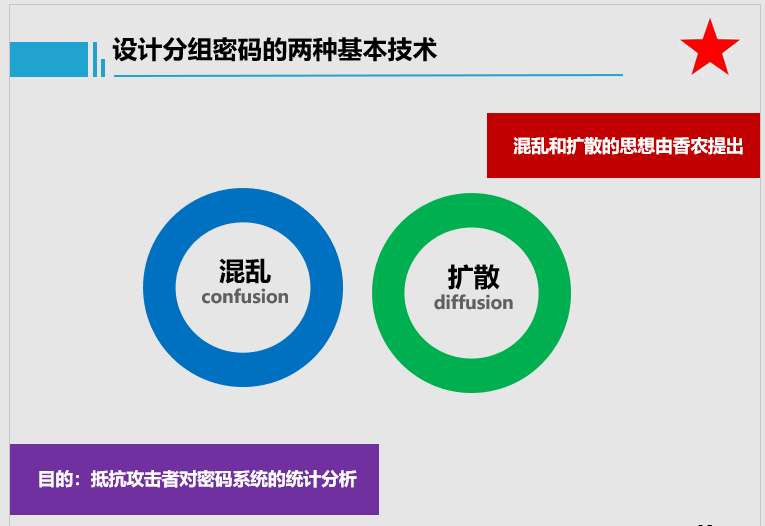




**密钥流生成器的用途 伪随机序列发生器**

* + **攻击者可能尝试重构生成密钥流的种子。**
  + **攻击原理：**
    - **攻击者完全可以知道你收集种子的方法(柯克霍夫斯原则)**
    - **如果你使用的种子不够 “好”，就很容易被攻击者重构。**
    - **必须使用“好”的种子，使之具有不可预测性**





混乱：

**目的：**

**使明文和密文之间、密钥和密文之间的**

**相关统计特性极小化，从而使攻击者无法找到密钥**

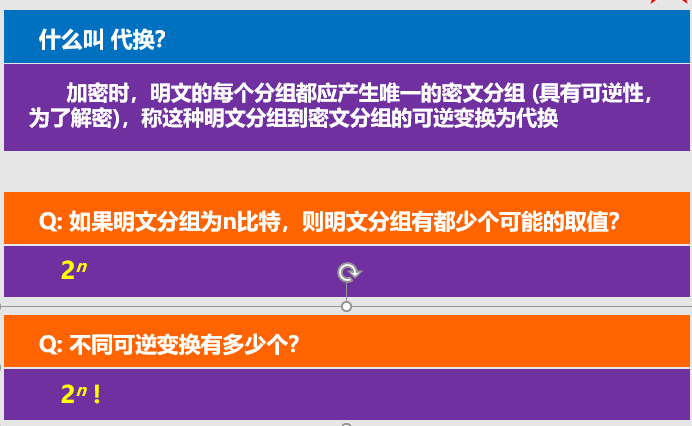
常用方法： 代换

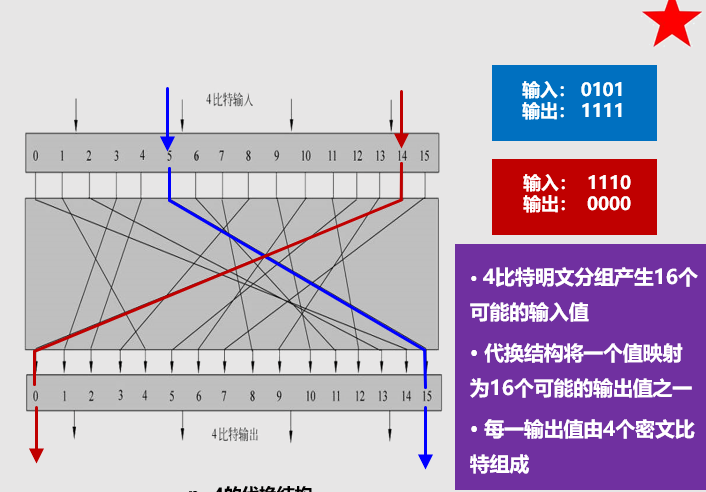
# 扩散

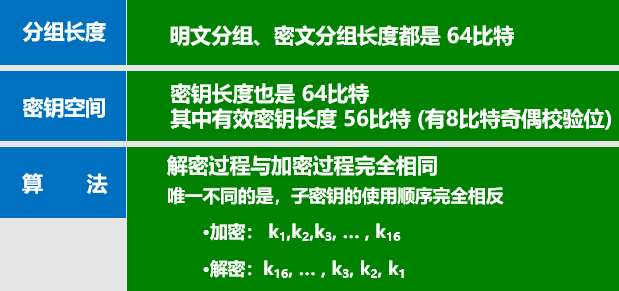
**目的：**

**将明文及密钥的影响尽可能迅速地散布到较多个密文比特中。**

常用方法： 置换



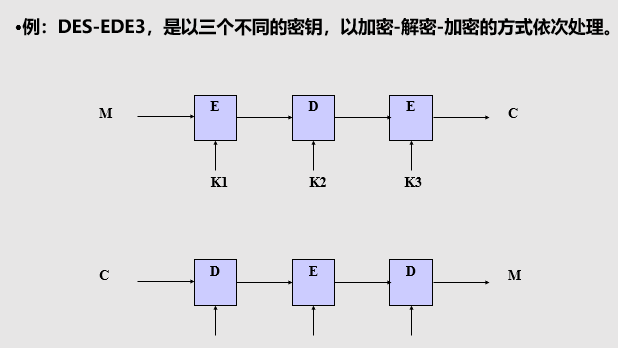




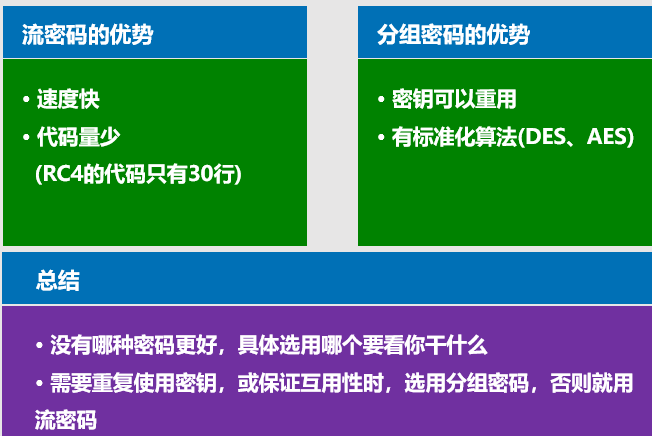
**数据加密标准 (DES) 针对DES的攻击**

* **差分密码分析**
  + **1990年，以色列密码学家E.Biham和A.Shamir提出，可对DES进行选择明文攻击。**
  + **该成果主要是理论上的。因为它所要求的时间量和数据量超出每个人的承受能力。**
  + **因此如果正确实现DES算法，对差分密码分析仍是安全的。**
  + **为什么DES能抵抗差分密码分析呢？**
    - **设计者早在差分密码分析法公布于世之前就已经知道了这种攻击方法。**
* **穷举密钥攻击**
  + **由于DES的有效密钥长度只有56比特,因此考虑穷举密钥攻击还是很靠谱的。**
  + **1999年1月，电子前沿基金会(Electronic Frontier Foundation)仅用22小时15分钟，就宣告破解了一个DES的密钥。**





**流密码与分组密码的比较**

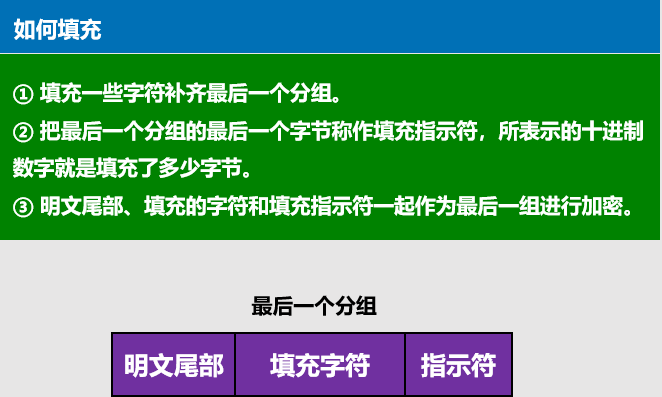




# 填充

**Q: 通常，明文长度是不固定的，按固定长度分组时，往往最后一个分组长度不足，如何解决？**

方法：填充。



**不论最后一个分组长度是否足够，都要进行填充**



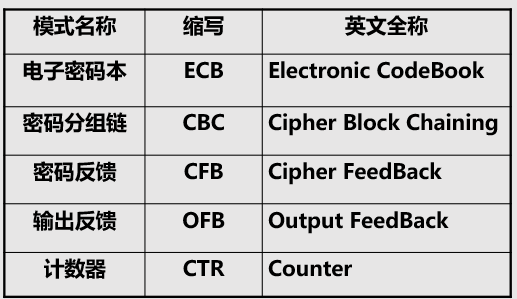
**Q: 为什么需要工作模式？**

**分组密码的输入是一个明文分组，是定长的。**

**要加密的明文是变长的，长度往往大于一个明文分组。**

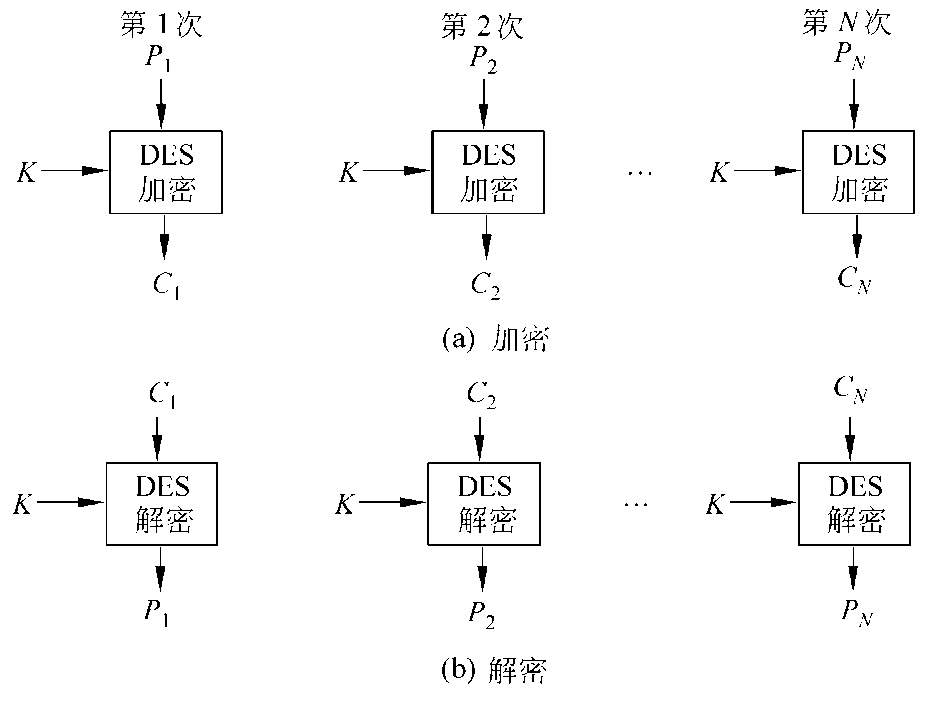
**即使有了安全的分组密码体制，也需要采用适当的工作模式来隐蔽明文的统计特性，以提高整体的安全性。**

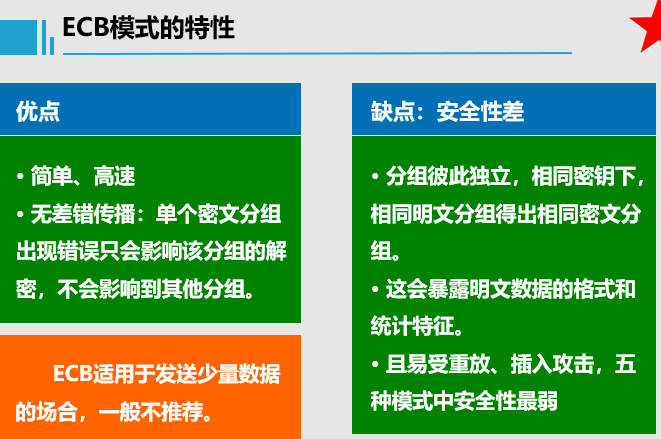
五种工作模式



**电子密码本模式 ECB**

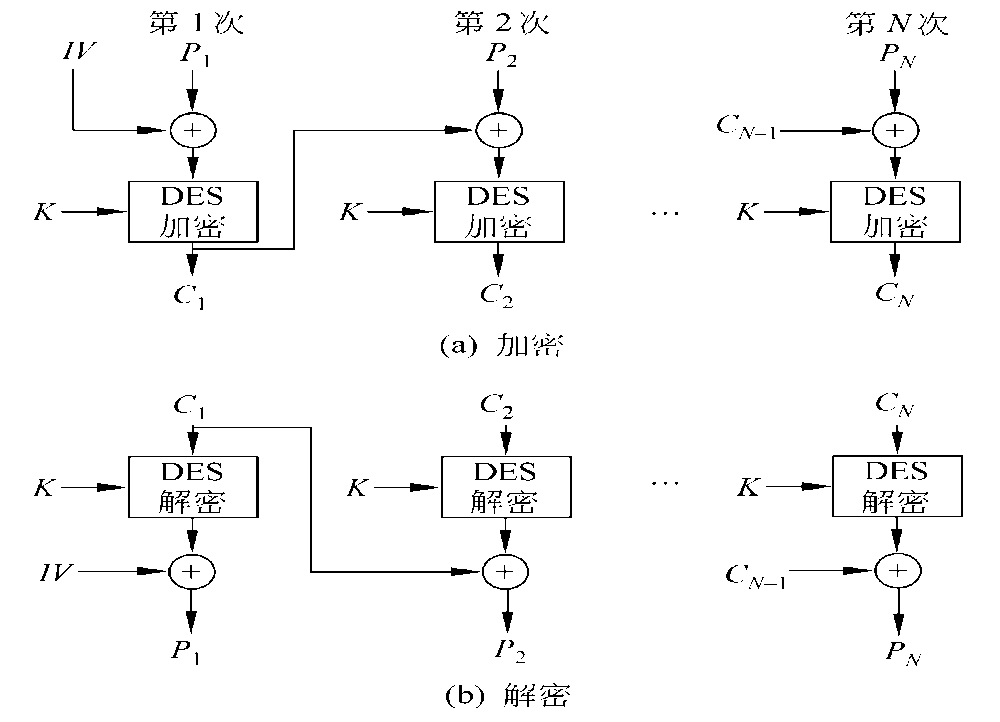
* 每个明文分组独立加/解密

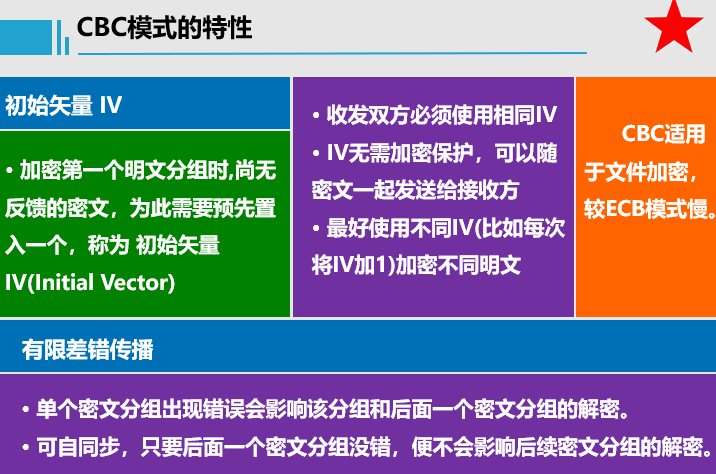




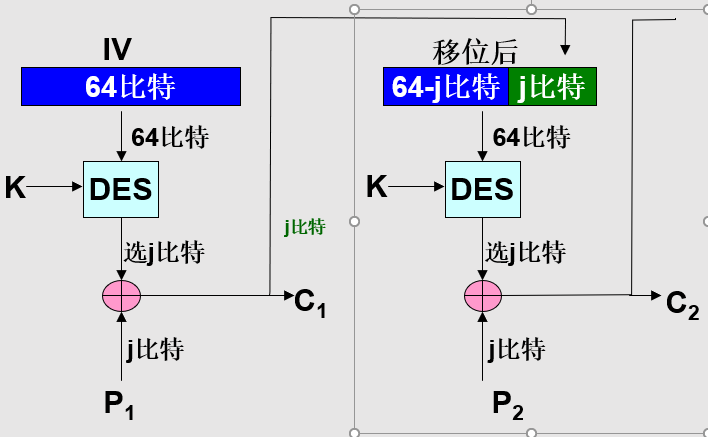
**密码分组链模式 CBC**

* 每个明文分组先与前一密文分组异或，再进行加密





**密码反馈模式 CFB**

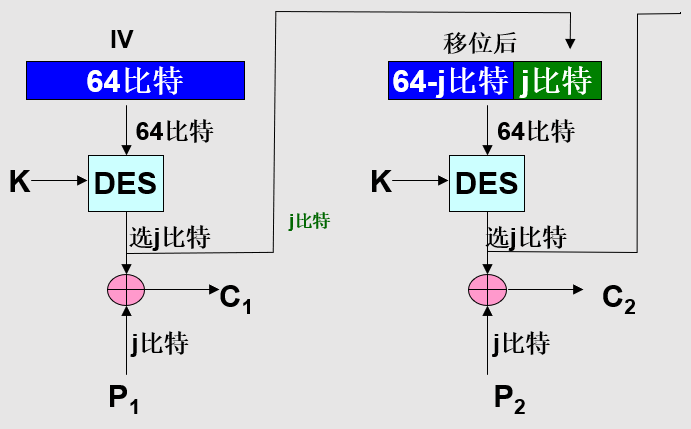


**CFB适用于 明文按字符(如电传电报)或按比特处理的流密码中**

**CFB适用于 无延迟的加密和传播**

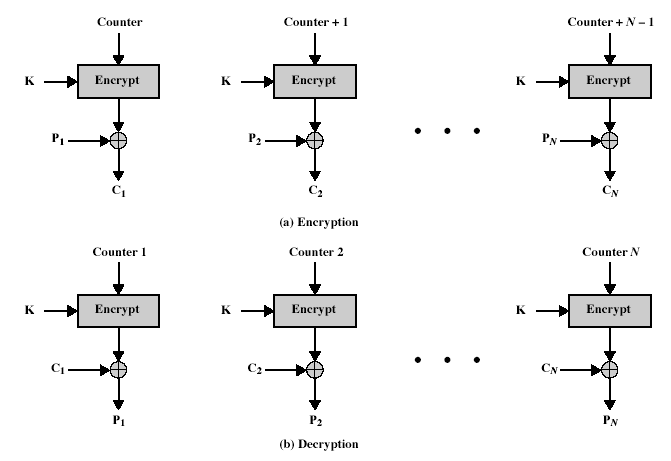
**CFB适用于 容忍以少量错误扩展换来恢复同步能力的场合**

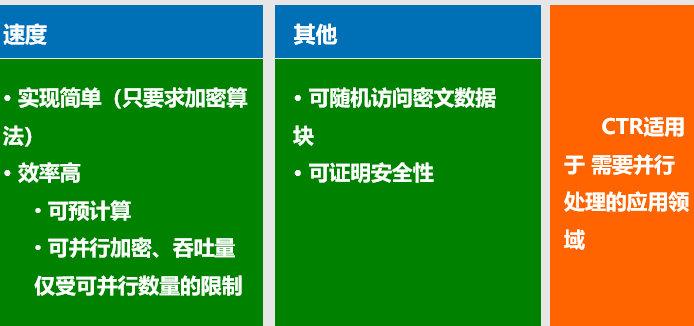
**输出反馈模式 OFB**



**OFB适用于 必须避免错误传播的高速同步系统**

**计数器模式 CTR**





**保护密钥是很重要的，因为所有的安全性都依赖于密钥的机密性**

**(柯克霍夫斯原则)**

**Q: 是否可以记住密钥，这样就不用存储，别人也偷看不了？**

**理论上可以，但不实际，因为密钥是随机的，很难记忆**

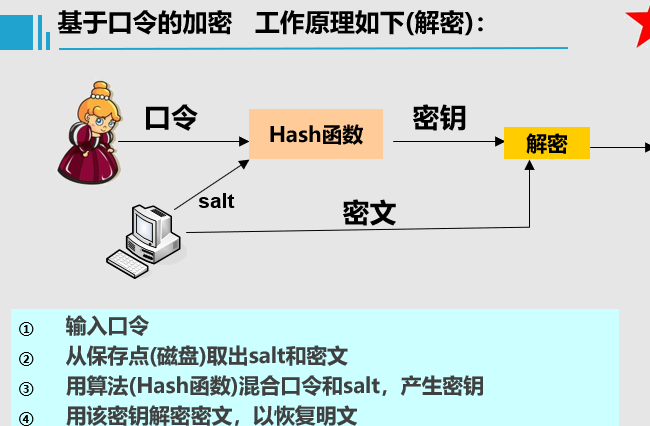
**Q: 既然有地方安全保存密钥，为啥不直接把敏感信息放在那里？**

**保护短的密钥比保护数以兆计的信息更容易**

**对称密钥的管理策略**

**用 密钥 保护数以兆计的信息，用一些其他技术保护大约16字节(128bit)的密钥**





**Q: 为什么不直接用口令作密钥？**

**口令的熵很小，远达不到密钥所要求的随机程度**

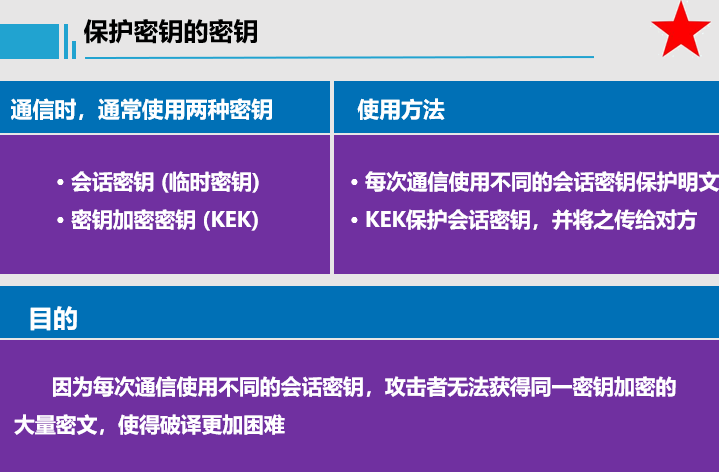
**Q: salt (盐值) 是干什么用的？**

**目的：为防止字典攻击中的预计算。**

**如果密钥仅由口令生成，攻击者可创建一个常用口令表 (字典)，对里面所有口令预计 算密钥。每次使用时就尝试这些密钥。字典可从黑客网站下载，也有很多发动字典攻击的软件**

**Q: 为什么salt和密文一起保存，保密salt不是更安全？**

* **使用salt的唯一目的是防止字典攻击中的预计算，而不是增加安全性。**
* **即使salt不保密，仍能达到目的。**
* **此外，如果保密salt的话，还不如直接保密密钥。**



**Q: 用KEK保护会话密钥，用什么保护KEK？**

* **使用 基于口令的加密，步骤如下：**
  1. **用口令和salt产生KEK。**
  2. **用KEK加密会话密钥，用会话密钥加密明文**
  3. **记住口令，保存salt和加密后的会话密钥。**
  4. **将密文和加密后的会话密钥传给对方。**
  5. **至于KEK，丢掉就OK了。**

**Q: 假设攻击者闯入你的电脑，偷走salt和密文(或 加密后的会话密钥)，他如何计算密钥？**

**方法一**

**穷举攻击密钥**

**(无需salt 也可以发动)**

**方法二**

**字典攻击 (猜测口令)**

**因为salt不保密，如果攻击者获得了salt，他仍能发起字典攻击，只不过要多花一些时间。**

**构造或下载一本常用口令的字典，然后尝试每个口令和salt产生的密钥。**

**两种攻击方法的比较**

**相比之下，字典攻击速度更快。但若口令不在字典里，当然不会成功**

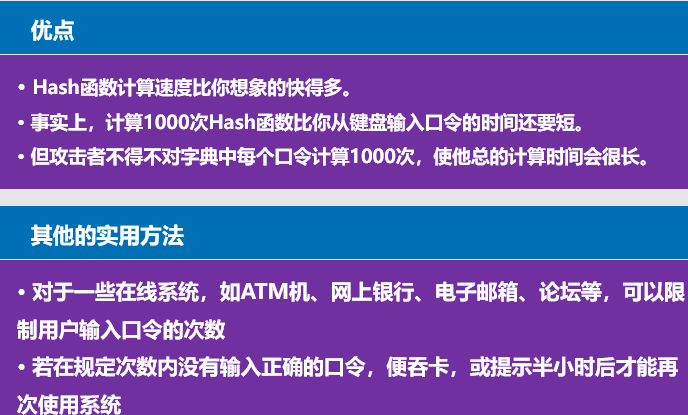
**一个聪明的攻击者一般会这样做：**

**首先尝试字典攻击，失败后换用改进的穷举密钥攻击。**

如何抵挡字典攻击？

基本思想：想办法降低攻击者的计算速度

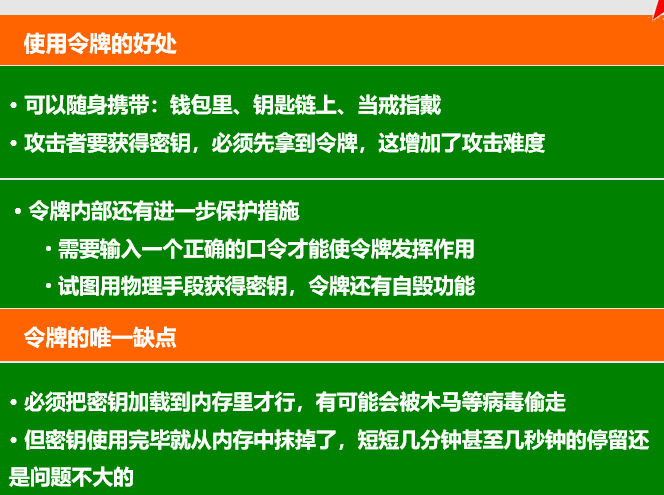
基本方法：**Hash函数混合salt和口令后，将输出再次用Hash函数混合，重复进行多次，假设1000次。**



**基于硬件的密钥存储**

**把密钥保存在一个硬件设备上**

* + - * **令牌**
      * **密码加速器**





**生物统计学方法并不总是靠谱**

* 生物统计学公司正在尝试制造相应的硬件，但至今未得到广泛应用，原因有二
  1. 设备的价格
  2. 可靠性:是不是总能正确地提取出身体特征？
* 但令牌不存在这些问题，它总能100%的工作

# 习题：

1. 流密码体制由 ( D ) 两部分组成

A. 驱动部分、反馈函数 B. FSR、反馈函数

C. FSR、非线性组合部分 D. 驱动部分、非线性组合部分

2. 设计分组密码的两种技术是 ( C )

A. 置换和移位 B. 易位和置换

C. 混乱和扩散 D. 隐写和扩散

3. ( D ) 不是分组密码的工作模式

A. CBC B. OFB C. CTR D. PBE

4.下列哪个不是分组密码体制 ( D )

A. DES B. AES C. IDEA D. RC4

5.下列哪种模式的安全性最差 ( A )

A. ECB B. CBC C. OFB D. CFB

6. CBC模式中，一个密文分组传输错误，会影响( B )个密文分组的解密

A. 1 B. 2 C. 3 D. 4