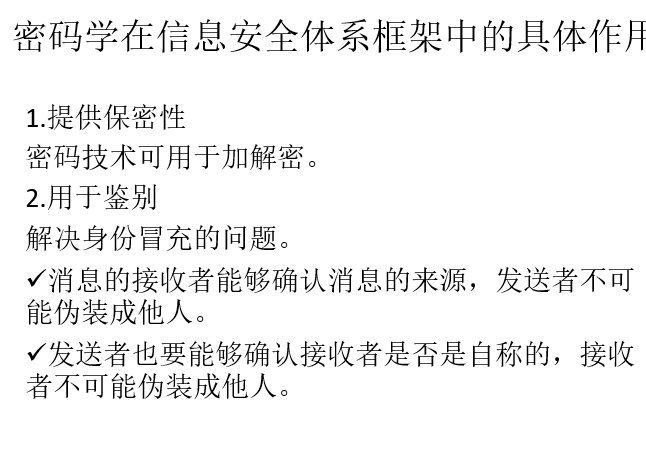
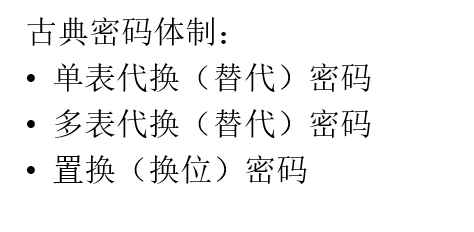
# 第一章

**密码学在信息安全体系框架中的具体作用**



# 第二章

**密码算法概念考，计算不考（到60页全看）**

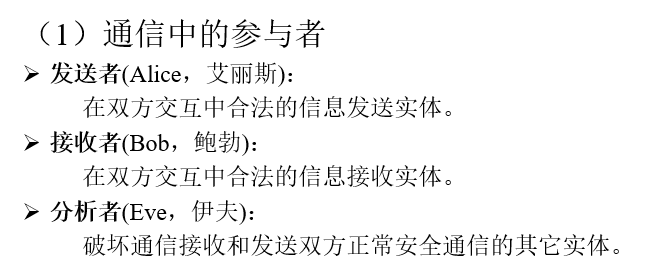


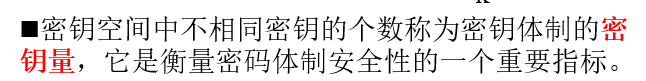
# 第三章

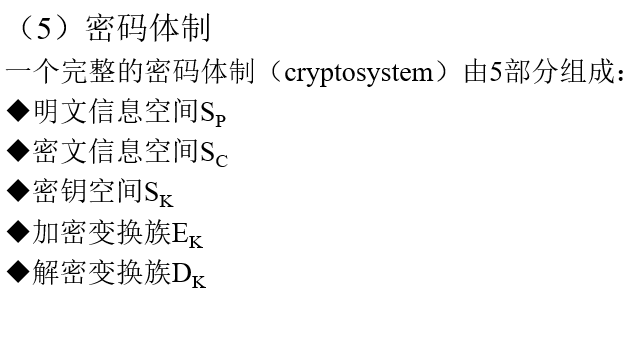
**概念全看**

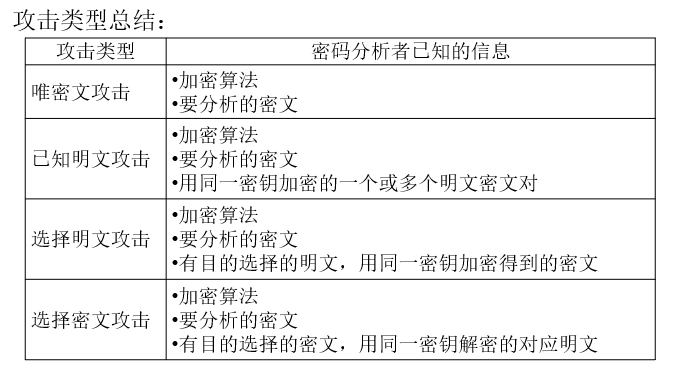
密码学(Cryptology)：是研究信息系统安全保密的科学。

* 密码编码学(Cryptography)：主要研究对信息进行编码，实现对信息的隐蔽。
* 密码分析学(Cryptanalytics)：主要研究加密消息的破译或消息的伪造。









评估密码系统安全性主要有三种方法：

无条件安全性

计算安全性

计算安全性又称为**实际安全性**。

**密码系统要达到实际安全性，满足以下准则**：

1. 破译所需的实际计算量（包括计算时间或费用）十分巨大，以至于在实际上无法实现。
2. 破译所需的计算实际超过被加密信息有用的生命周期。如战斗打响的命令只需保密到战斗打响前等。

3 破译所需的费用超过被加密信息本身的价值

**分组密码(block cipher)：**将明文分成固定长度的组，用同一密钥和算法对每一块加密，输出也是固定长度的密文。

**流密码(stream cipher)：**又称序列密码。序列密码每次加密一位或一字节的明文，也可以称为流密码

**对称密码体制**

加密密钥与解密密钥同：*K*1*=K*2

**非对称密码体制**（公开密码体制）

加密密钥与解密密钥不同：*K*1*≠K*2

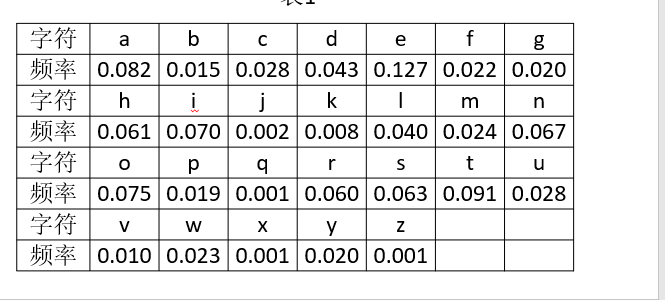
# 第四章

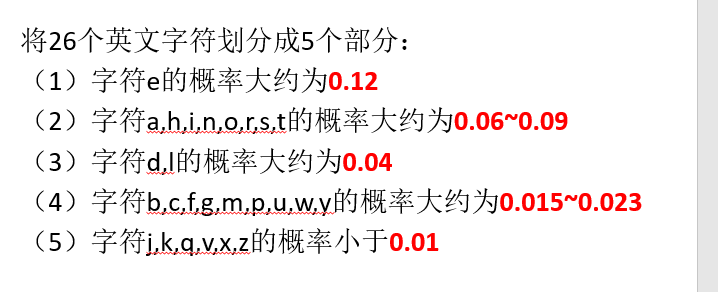
**概念**

**具体分析，破解过程不考**

**用了什么攻击方法，为什么…攻击方法好**

英文字母的频率特性





单表代换密码的统计分析

仿射密码体制的攻击

多表代换密码分析

：Kasiski（卡西斯基）测试法

* 基本思想：当用给定的n个字母周期性地对明文字母加密，通常情况下，相同的明文字母将对应不同的密文字母。但是，当两个相同的明文段在明文序列中间隔的字母数为n的整数倍时，将加密成相同的密文段。

重合指数法

思路：完全按照语法规则形成的英文文本中字母重复出现的频率与完全无意义的英文文本（如多表代换加密形成的密文）中字母重复出现的频率显然存在差别

在古典密码的分析中， Chi-测试：

（1）可用来确定是否采用了相同或不同的代换

（2）简化多表代换为单表代换

故Hill密码能较好地抵抗字母频率的统计分析，采用**唯密文攻击**较难攻破，但采用**已知明文攻击**容易破译

# 第五章

**数论不直接考，如果加解密算法中用到的考**

**算数基本定理，欧拉定理，欧几里得定理**

**复习看书后**

# 第六章

**分组密码DES概念**

**设计原则（核心思想）**

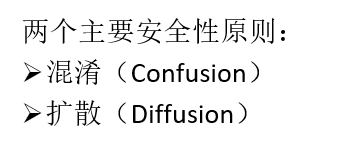
**结构2Fesite考**

**密码算法具体分析，具体攻击不考，分析方法考**

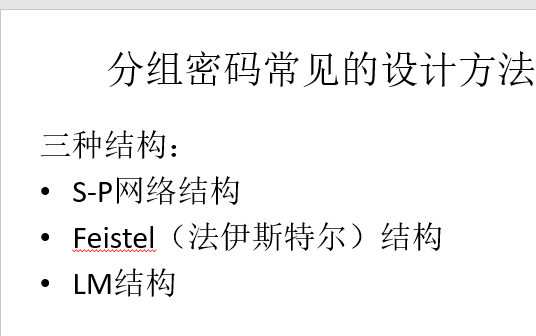
**证明循环群不考**

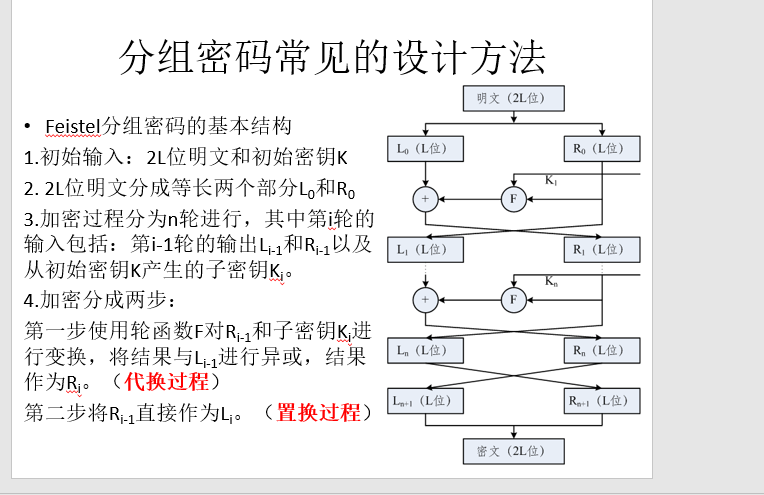
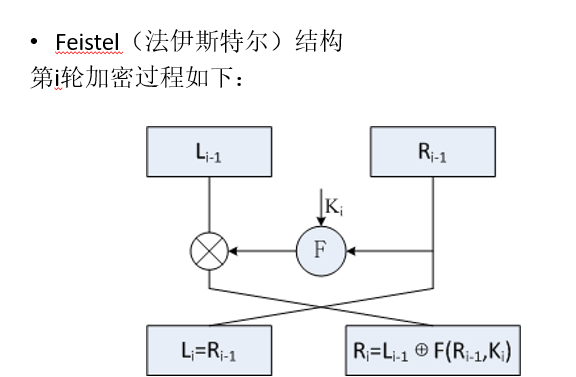
* 分组密码是对称体制，也就是加、解密的K相同
* 分组加密算法的主要特点
* 速度快
* 易于标准化
* 便于软硬件实现

设计原则



* 混淆是使密文的统计特性与密钥的取值之间的关系尽可能复杂化，以使密钥和明文以及密文之间的依赖性对密码分析者来说是无法利用的。
* 扩散的作用就是将每一位明文的影响尽可能迅速地作用到较多的输出密文位中，以便在大量的密文中消除明文的统计结构，并且使每一位密钥的影响尽可能迅速地扩展到较多的密文位中，以防对密钥进行逐段破译。



1.DES的雪崩效应

雪崩效应定义为：明文或密钥的一点小的变动应该使密文发生一个大的变化

2.S-盒的设计准则

问题涉及美国国家安全局（NSA）， NSA修改了IBM最初设计的S-盒，虽然仍然满足最初的S-盒设计原则。人们怀疑NSA在S-盒中嵌入陷门，使得NSA借助于这个陷门及56位的短密钥可以解密。

3.56位有效密钥太短

4.弱密钥和半弱密钥

如果对于初始密钥，所产生的子密钥都是一样，这样的密钥称为弱密钥。

若给定密钥k，相应的16个子密钥只有两种，且每种都出现8次，称为半弱密钥。至少有12个半弱密钥，组成6对

半半弱密钥：有些密钥只产生4种密钥，每种出现4次，称为半半弱密钥，共48个。

5.互补对称性

由于互补对称性，穷举攻击时仅需试验所有256个密钥的一半。

1. 穷举攻击

（1）尝试所有的可能情况

（2）字典攻击：明密文对编成字典，尝试字典中所有可能的情况

（3）查表攻击：表中是所有可能的明文。给定明文，用所有的2k个密钥加密，对比所得密文。是一种选择明文攻击。

2. 计时攻击

利用加密或解密算法对不同的输入所花费时间的细微差别，再通过对很多种密文解密所需时间的观察，可以获得密钥与明文的信息。

3. 差分密码分析

通过分析明文对的差值以对密文对的差值的影响来恢复某些密钥比特。

4. 线性密码分析

通过寻找一个给定密码算法有效的线性近似表达式来破译密码系统。由于每个密码系统都是非线性的，故只能寻找近似的线性表达式

# 第七章

**AES字乘法，加法原理，算法理解**

**分组密码的工作模式**

a(x)={03}x3+{01}x2+{01}x+{02}进行模x4+1乘法

a-1(x)={0b}x3+{0d}x2+{09}x+{0e}

分析

（1）在AES算法中，轮密钥生成算法的非线性性质消除了产生相同轮密钥的可能性。加/解密过程中使用不同的变换可以避免出现弱密钥、半弱密钥、半半弱密钥等。

（2）经过验证，AES能够抵抗所有针对DES的攻击方法的攻击，如部分差分攻击、相关密钥攻击等。

（3）到目前为止，最有效的攻击方法是穷举搜索攻击，因此AES是安全的。

AES特点：

* 不属于Feistel结构
* 加密、解密相似但不对称
* 支持128数据块大小
* 支持128/192/256密钥长度
* 有较好的数学理论作为基础
* 结构简单、速度快

AES设计原则

* 简单性

简单性便于分析理解是如何抵抗所有类型的攻击。

* 对称性

（1）各轮之间的对称性

各轮之间具有对称性，好处是在密钥的控制下对同一轮交换进行循环迭代，优点是只要描述一轮变换即可将整个规范描述清楚，另外，在软件实现中可仅对一轮进行编辑。

（2）轮变换内部的对称性

（3）D-盒的对称性

（4）S-盒的对称性

（5）加密和解密过程的对称性

* 对抗攻击方面

（1）选择差分均匀性比较小和非线性度比较高的S-盒

（2）适当选择线性变换，使得固定轮数中的活动S-盒的个数尽可能多。

优点是可以估计算法的最大差分特征概率和最大线性逼近概率，这样可以评估抵抗差分密码分析和线性密码分析的能力。

工作模式

电子密码本ECB模式（Electronic Codebook Mode）是最简单的模式。

密码分组链接模式（CBC）：加密算法的输入是当前明文分组Mi和上一次产生的密文分组Ci的异或

密码反馈模式（CFB）：

输出反馈模式（OFB）

计数器模式（CTR）

# 第八章

**公钥密码体制**

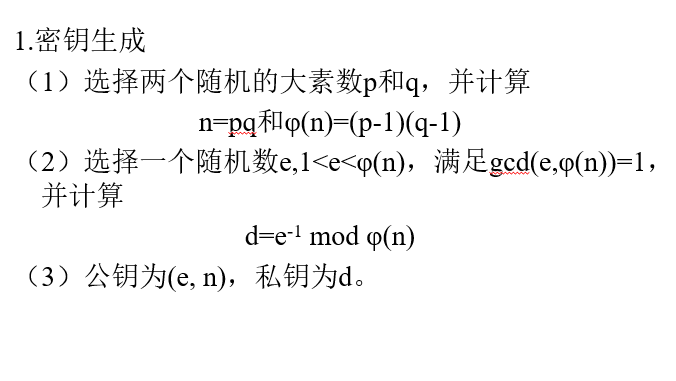
**产生大素数算法概念**

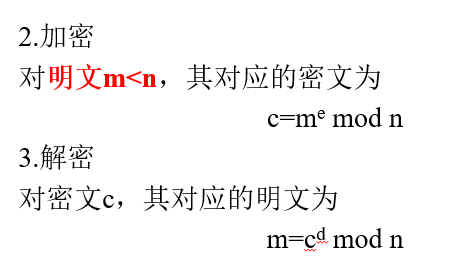
**安全性不考，应用不考**

**椭圆曲线密码算法**

**非确定安全算法**

RSA公钥密码体制





RSA应用中的问题

1.p与q的差必须很大

2.p-1与q-1的最大公因子应很小，以避免密文迭代攻击

3 不可使用公共的模n

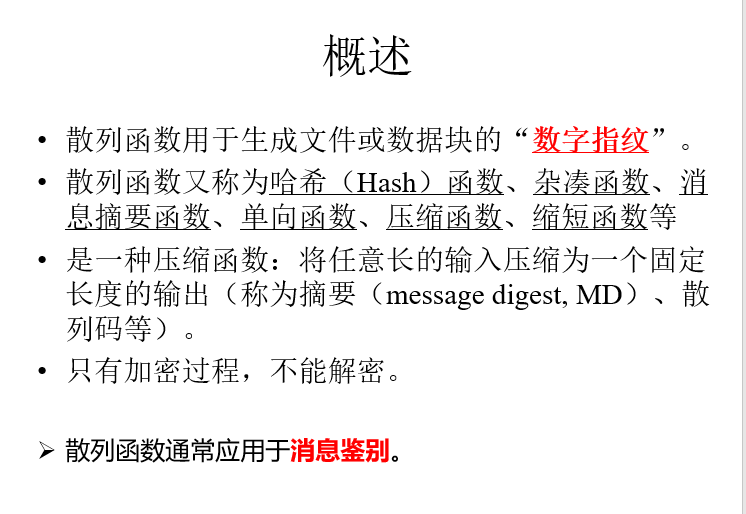
4.不仅要注意私钥d和大素数p、q的保密，还要保密φ(n)

5.避免不动点问题

# 第九章

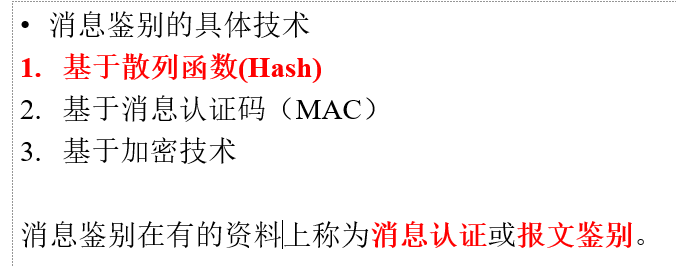
**散列函数意义，具体算法不考，考概念**

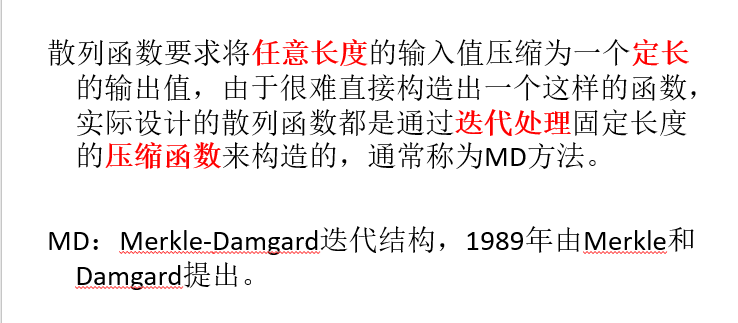
**生日攻击，消息鉴别理解**

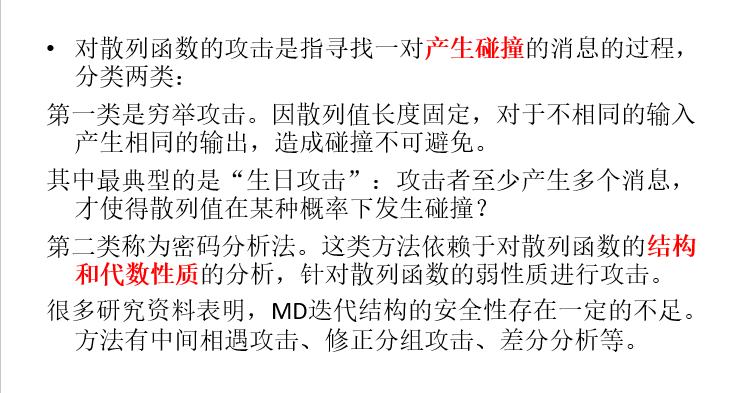


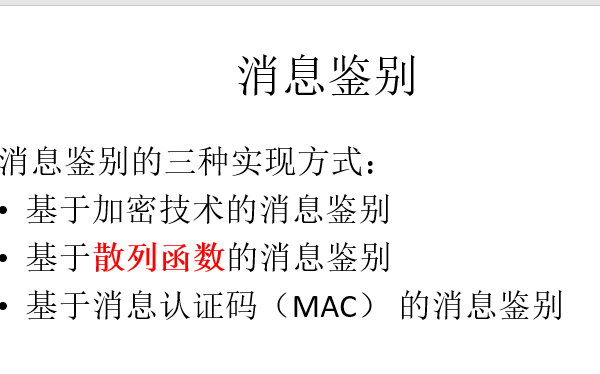
* 消息鉴别有三个主要目的

1. 验证消息的发送者是真正的（所声称的），而不是冒充的，即信源识别；
2. 验证消息的完整性，在传递或存储过程中未被篡改、重放或延迟等。
3. 抗抵赖





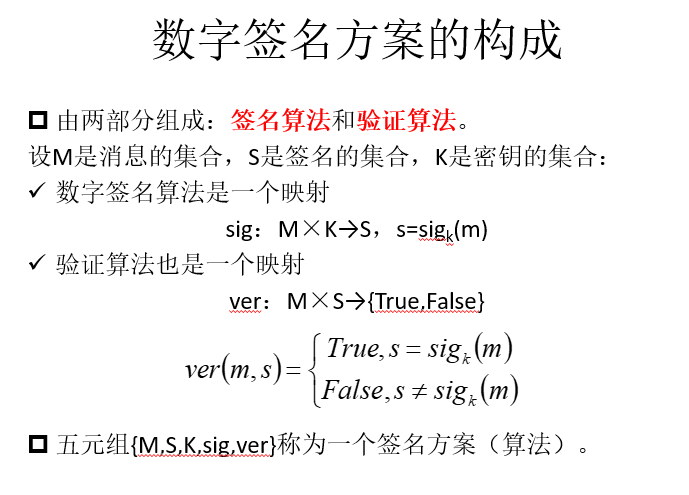




# 第十章

**数字签名，理解概念，流程**

**加解密算法的作业，理解概念**



# 第十一章

**密钥管理概念，可以看书**

**分发四张方式**

**协商不考算法**

**数字证书概念，原理**

**秘密分割方案考**

* 密钥管理是密码学的一个分支，是**密码学应用**最重要、最困难的部分。
* 密钥管理负责密钥从产生到最终销毁的整个过程（生命周期）中的一切活动，包括：密钥的生成、存储、分发、使用、备份/恢复、更新、撤销和销毁等。



* 密钥分发有两种方式：离线分发和在线分发
* 离线分发：通过**非通信网络**的其他物理渠道携带密钥进行分发。缺点：用户增多，密钥量将增加，密钥更新麻烦；不能满足陌生人之间的保密通信；成本高。
* 在线分发：通过计算机网络在线自动分发，需要一个密钥分发中心（KDC）来实现。

公开密钥的分发

1.公开发布

2.建立公钥目录

3.带认证的公钥分发（**在线服务器方式**）

4.使用数字证书的公钥分发（离线服务器方式）

# 第十二章

**序列密码，不考加解密**

**移位的例子要看懂，怎么算**

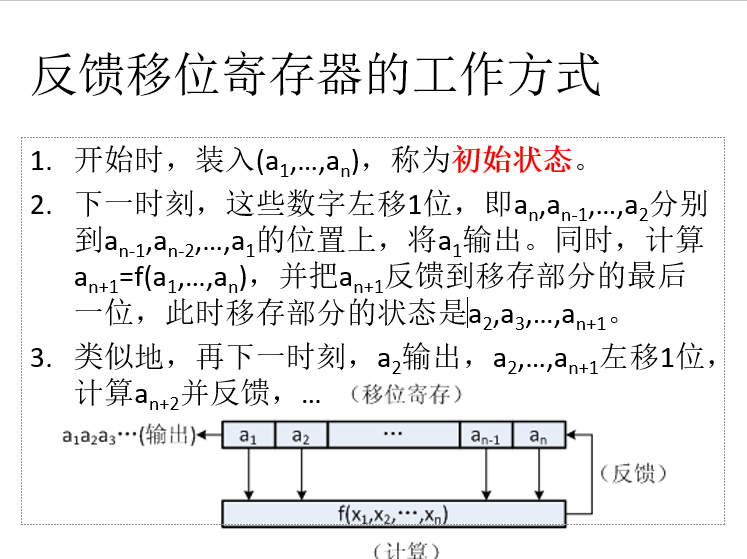
**序列性质理解，为什么有随机性**

**怎么产生伪随机序列**

**随机性假设的三个条件**

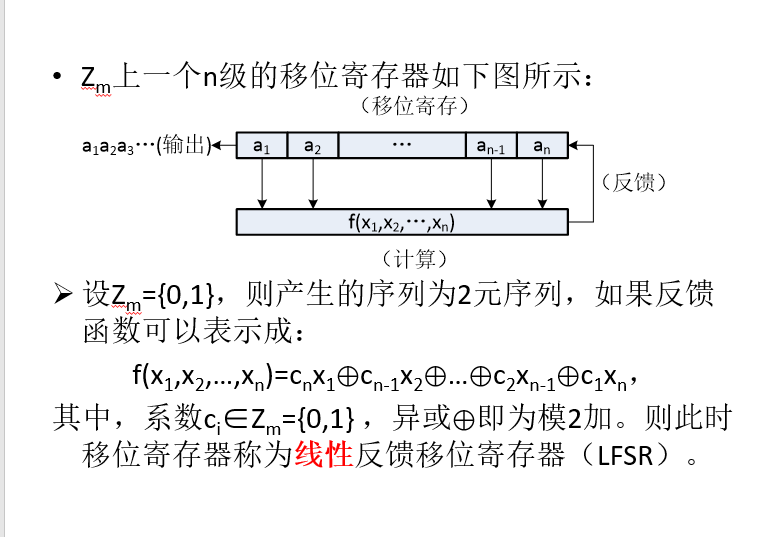
**一次一密**

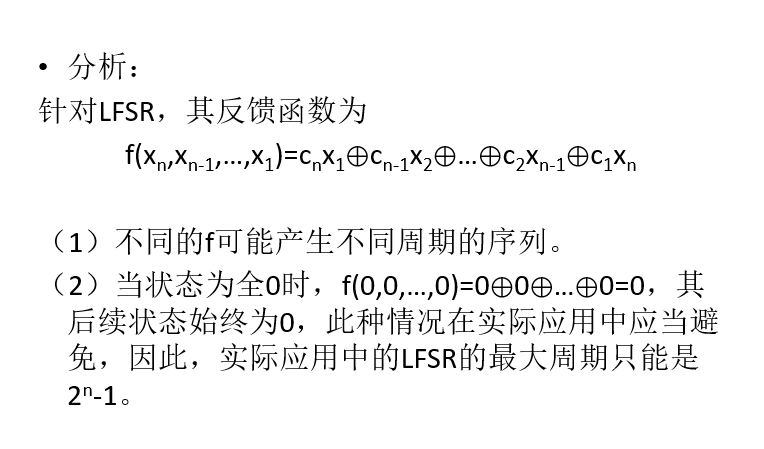
**RC4不考**

序列的性质分析

1.统计平衡特性

对M序列的分析表明，M序列具有**良好统计平衡**特性，是一种性能优良的伪随机序列，作为流密码加密的密钥流，难以破解。

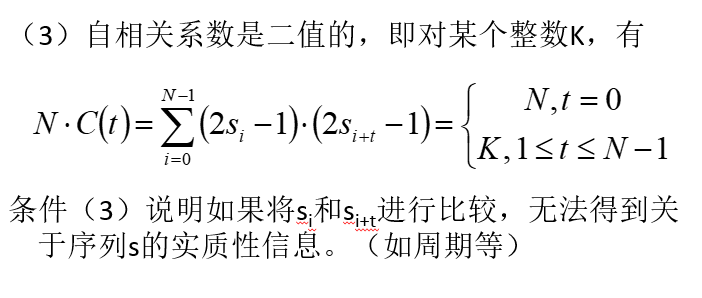


随机性假设的三个条件

1 在序列的一个周期内，0和1的个数至多相差1.

2 在序列的一个周期内，长为1的游程个数占总游程数的1/2，长为2的游程个数占总游程数的1/22，类推，长为i的游程个数占总游程数的1/2i，且在等长的游程中，0游程和1游程各占一半。

说明在已知位置n前若干位置上的值的前提下，在第n个位置上出现0和1的概率是相等的；

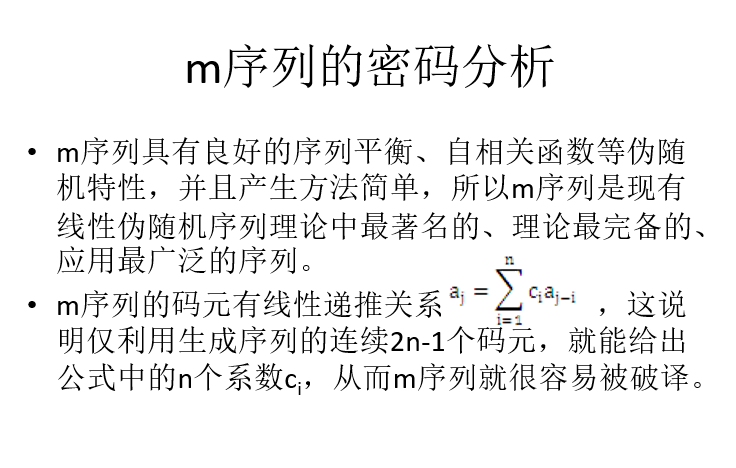


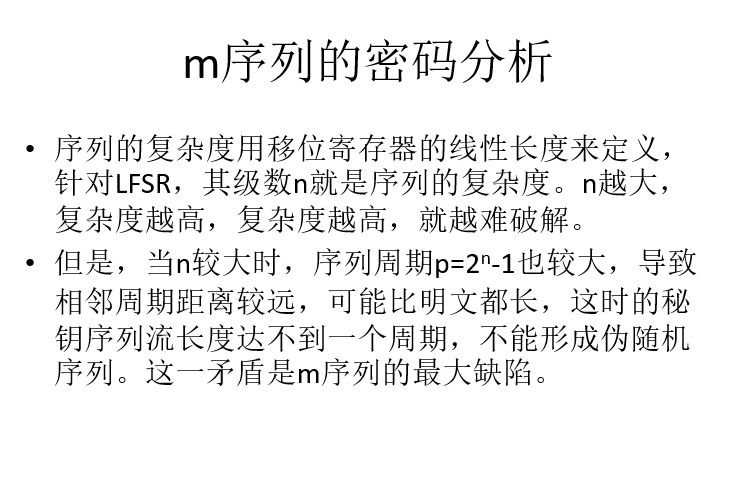
m序列的统计平衡特性

m序列的移位相加特性:

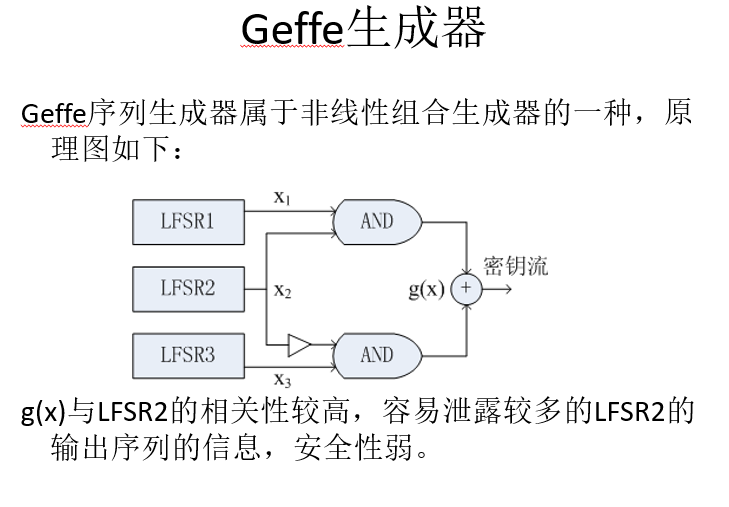
一个m序列与其经任意次延迟移位产生的另一个**不同**序列模2相加，得到的和序列仍是该m序列的平移等价.

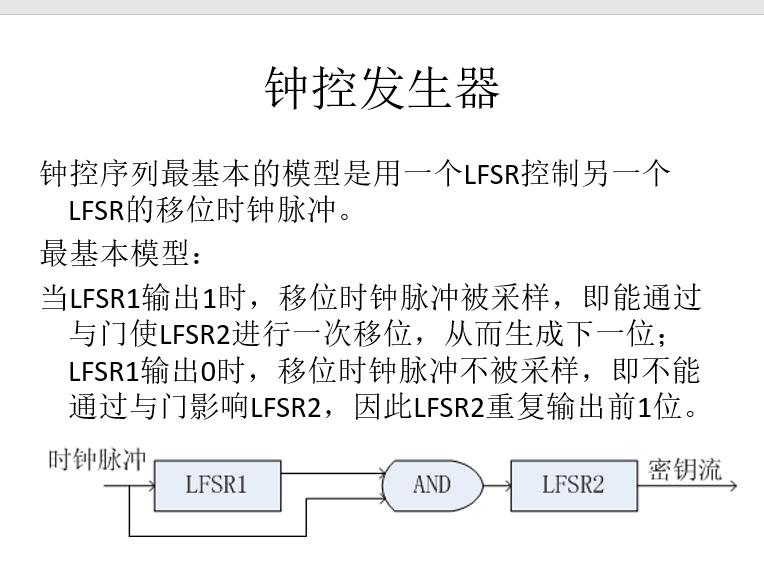
二进制m序列具有双值自相关函数特性。

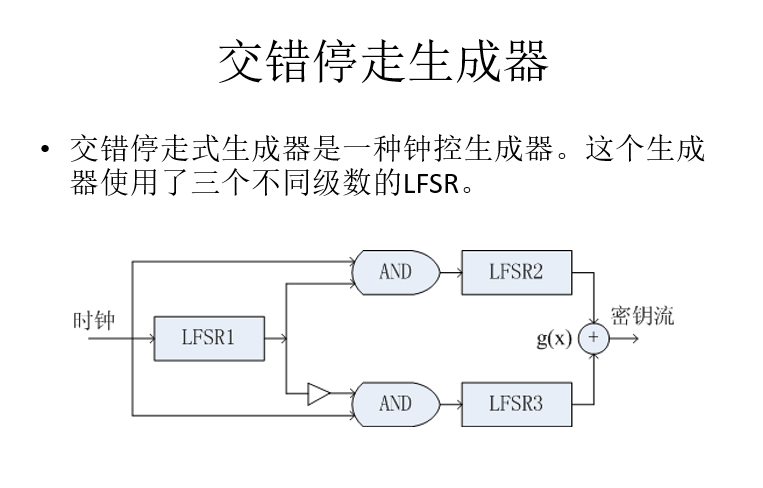


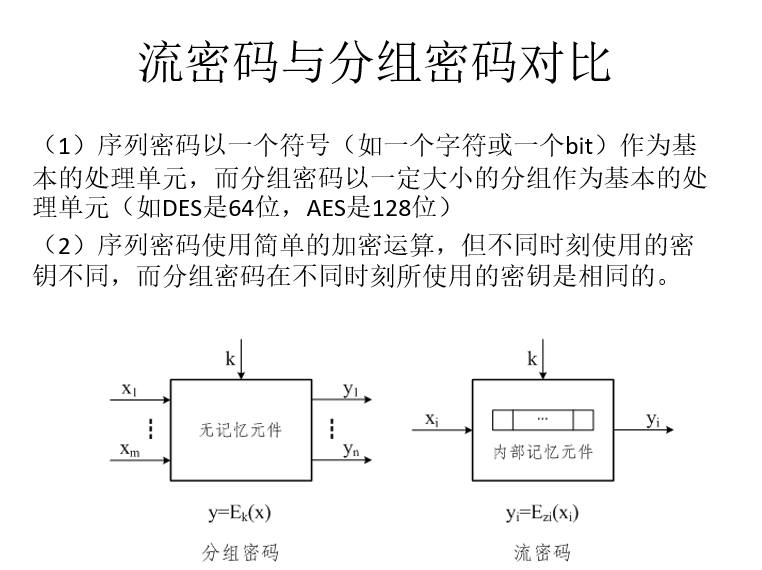
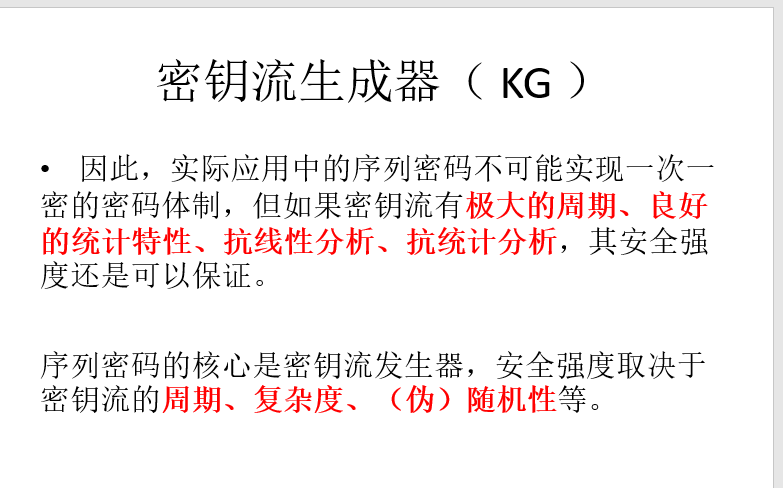


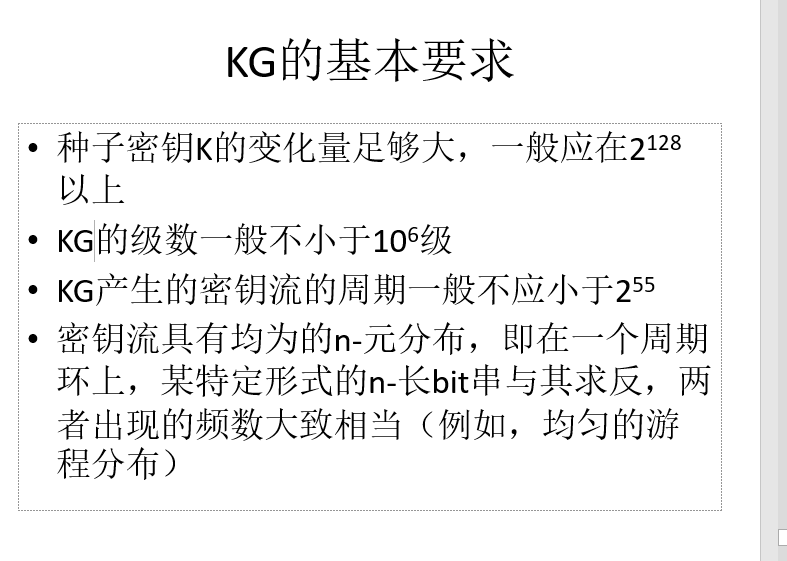
基于LFSR的非线性组合的  
序列密码









**考试题型**

**选择，填空，计算，可能有简答。**