2023-2024-2《应用密码学》复习提纲

* 第一章（ 1.3, 1.4 ）
  1. 密码学的基本概念（10）

密码编码学，密码分析学，密钥密码学

密码体制构成（五元组）

M，C，K，E，D

分类

执行操作方式：替换和换位

收发双方密钥是否相同：对称和非对称

分组和序列，序列还与密文在明文中的位置有关（15）

2、分析密码算法的方法、密码体制攻击方法（唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击和选择文本攻击）

* 第二章（2.3）

1. 古典密码的基本概念
2. 替换密码和换位密码的基本概念 （替换：摩斯密码、单字符单表替代（凯撒、 仿射）、多字符多表替代（维吉尼亚、Hill）。换位：滚筒密码，列换位密码）

3、仿射密码，维吉尼亚密码加密和解密过程

4、古典密码的安全性分析

* 第四章（4.1, 4.2，4.3, 4.4, 4.7）

1、分组密码基本概念、原理，常见的对称密码算法DES、AES等，国密SM4算法的分组长度，密钥长度等

2、DES算法、AES算法的相关概念（密钥长度、分组长度、轮次等）

3、多重DES算法密钥长度 (三重 EDE2 EEE3 )

4、DES算法轮结构（S盒），AES算法整体结构、AES算法四个基本变换（S盒等），有限域上字节的表示、基本运算（16进制和2进制的转换）

5、分组密码算法五种基本模式（ECB、CBC、CFB、OFB、CTR）的加解过程、特点、差错传播、特性比较等

* 第五章（5.2, 5.3）

1、序列密码分类（同步序列密码和自同步序列密码）

2、线性反馈寄存器（线性反馈移位寄存器的反馈函数，特征多项式，周期，输出序列，m序列）

* 第六章（6.1、6.2）

1. 非对称密码概述（分类：基于大整数因式分解困难性问题、基于离散对数困难性问题、基于椭圆曲线离散对数困难问题等等，对称密码算法和非对称密码算法区别）
2. RSA算法（密钥生成、加密和解密）模幂运算（Fermat小定理，模重复平方，欧几里得扩展算法求逆），RSA算法安全性 RSA加密解密实现（第2次实验）
3. 对称密码和非对称密码区别

* 第七章（7.1，7.2, 7.3.1，7.5）

1、Hash函数概念和安全性要求、MD5算法的概念、SHA系列和国密SM3算法的摘要值长度

2、SHA-1算法（算法流程、SHA-1数据填充和数据扩充（ASCII码、16进制和2进制的转换）

3、消息认证（消息认证、消息认证码、基本概念、三种使用方式（206页））

* 第八章（8.1, 8.2, 8.3.1）

1、数字签名原理

2、数字签名分类

3、RSA数字签名算法

* 第九章（9.1）
* 1、认证协议(单向认证协议和双向认证协议、有无第三方参与）的理解

2、认证模型和保密通信模型的理解

3、身份认证技术（概念及几种常见的认证技术）

* 第十章（10.1, 10.2, 10.3, 10.5.1 10.5.3）

1. 密钥组织结构和密钥分类（基本密钥、主密钥、密钥加密密钥、会话密钥）
2. 密钥管理的内容

DH密钥协商协议（协议执行过程、中间人攻击）、STS协议（如何防止中间人攻击）

考试题型

一、选择题（30分，2分/每题，15题），

二、判断题（10分，1分/每题，10题）

三、填空题（10分，1分/每空，10空）

四、简答和计算（30分，6分/每题，5题）

五、综合计算题（20分，10分/每题， 2题）

计算题整理：

（1）密钥共享计算：在复习ppt第234页，若想要防止中间人攻击，则使用240页的方式，使用计算出的K对签名进行加密并发送给A

（2）SHA-1的消息分组处理的计算，要注意最后一个填充分组是由消息长度+1个bit的“1”+填充的“0”+64bits的消息定长表示的，总共相加=512bits。{填充时0的个数要取最小的非负整数}，消息扩展时，W[t]=ROLT循环左移(W[t-3]异或W[t-8]异或W[t-14]异或W[t-16])，都是下标的计算。

（3）**RSA**算法的计算：选取e、p、q，计算n=pq，并求出n的欧拉函数值。根据ed同余1mod （n的欧拉函数值），c同余m的e次方mod n，m同余c的d次方mod n，进行计算几个参数的值。还有签名值的计算，签名加密时s同余m的d次方mod n，解密时m同余s的e次方mod n。

（4）序列密码线性移位寄存器的计算。反馈移位寄存器：包含反馈函数，特征多项式（也叫连结多项式，注意一定有一个+1在结尾），有限域上的多项式等多个专业术语。计算方式是将反馈回路看作开关，为1接通1为0断开。在计算时还需要写出状态转换表来求出周期。

（5）DES的计算考得不多。但和AES差不多的，E盒扩展，与轮密钥做异或，S盒压缩，P盒置换，输出32bits。E盒扩展就是先把原消息列成4\*8的矩阵，然后在两边按照要求扩展即可，要注意是否是16进制输出，需要按照要求进行输出。S盒压缩就是b1b7决定行，b2b3b4b5决定列。P盒置换就是查表。

（6）AES相关计算：

轮密钥加：矩阵对应元素做异或即可

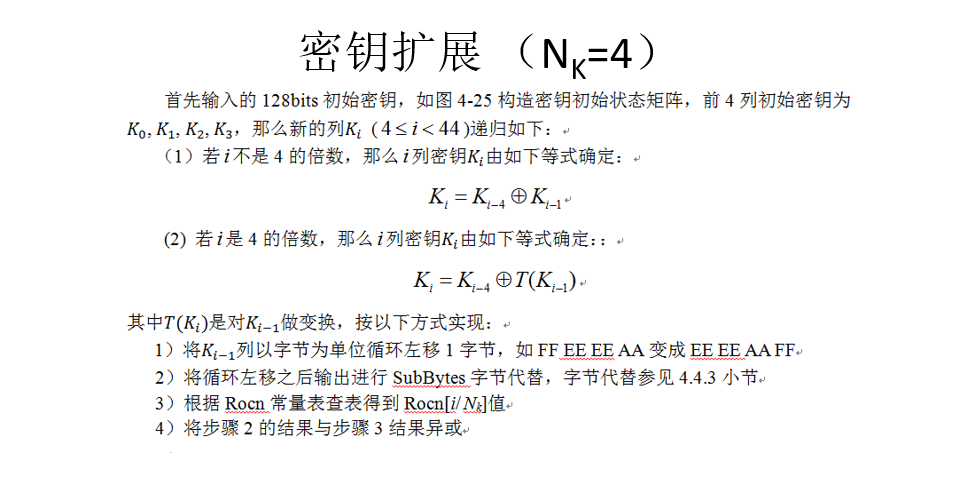
字节代替：16进制查表，假设是0x03H，则第0行第3列；0x34，则第3行第4列

行移位：第一行不动，第二行循环左移1个字节，第三行循环左移2个字节，第四行循环左移3个字节。

列混合：明文输入矩阵每个元素与固定矩阵做矩阵的乘法。

有限域x乘：\*{02}相当于循环左移1位，但要判断最高位b7是否为1，若b7=1，则在左移位后还要与{1B}做异或。

密钥扩展：记住原有多少个密钥分组，128为4个，192为6个，256为8个，每个分组32bits，公式是轮密钥长度128bits\*（轮数+1）=总共密钥bit数。要除以32算出分组数，然后减去原有分组才能得到扩展的分组数。

密钥扩展的计算：

**第10章：（估计15分左右，重点是密钥分类、密钥协商的计算和中间人攻击的详细过程。）**

（1）使用层次化的密钥结构，方便管理，相互控制。

（2）密钥分类

基本密钥：又称初始密钥或用户密钥，可以较长时间标识特定的一对用户（可以理解为一次会话双方中产生的公钥私钥共4把密钥的结合）

会话密钥：又称数据加密密钥，用于加密会话的数据。

密钥加密密钥：用来加密密钥的密钥，又称二级密钥

主密钥：使用周期最长，最高层次的密钥。

（3）密钥管理的内容：密钥的生成、使用、存储、备份、恢复、更新、销毁以及密钥撤销等。

（4）管理方式：层次化的密钥管理方式

（5）密钥共享计算：见计算题归纳。

（6）密钥分配方式：集中式分配和分布式分配。

**第9章消息认证（重点是单向和双向的过程以及每一步认证了谁的身份）：**

（1）认证的定义：核实真实身份的过程，主要作用是弄清楚对象是谁，要使用有特殊特征，能够标志一个对象。

（2）认证的分类：单向认证和双向认证。

单向：主要代表有电子邮件，有点事无需双方同时在线，只需要将数据保存下来即可。

单向认证又分为两种：

需要第三方的单向认证和不需要第三方的单向认证。

需要第三方的：过程如下：A向kdc申请会话密钥，告诉他IDA和IDB。接下来KDC向a反馈他的公钥和加密后的会话密钥以及B的公钥等信息。A再用B的公钥将共享密钥数据加密发送给B。此过程中第三步实现了A对B的认证。

不需要第三方的单向认证：

直接将共享密钥用B的公钥加密后发送给b就可以，如果有相应的信息则一起加密。

双向认证：AB相互认证，过程如下：

（1）A想要B的公钥，所以将IDa、IDb和随机数N1（保证完整性）发送给kdc告诉他我是a，想要和b通信，请你给我分配会话密钥。

（2）kdc将会话密钥，随机数N1和用Ekb加密后的ks和ida发送给A，A进行的行为是解密然后获得共享密钥以及B的ID

（3）A解密后，将剩下的KB加密后的IDA和ks发送给b，此时只有正确的B才能解锁并查看信息，所以A在此过程中认证了B的身份。B在收到信息后进行解密，得到Ida和KS

（4）B选取一个随机数N2，然后用共享密钥加密后发送给A，只有正确的a才能使用共享密钥进行解密查看。

（5）A收到b发来的N2后，利用函数算法计算后发送给B，既保证了消息完整性，也让 B成功认证了A的身份。

但是即使是双向认证，也容易遭受到重放攻击（攻击方式是A使用过期的密钥与B进行简单的重放攻击，除非B能一直记住A使用的密钥，否则会遭到攻击），解决办法为在消息中加入时间戳。

在复习ppt第220多页

**第8章数字签名**

（1）数字签名的产生：s同余m的d次方mod n （m，s）参数构成对消息的签名。

（2）验证过程：收方利用m同余s的e次方 mod n来验证此消息是否为BOB发送的。

（3）缺陷在于得到同一个人对不同消息的两次签名后可以计算出两次签名的乘积。这就导致了RSA算法的缺陷。

（4）怎样利用数字证书实现信息安全？ppt214页

加密过程如下：

1.发送方先根据信息生成数字摘要

2.用私钥签名。签名后将得到的签名，信息和数字证书三个东西进行对称加密得到加密后的信息。

3.再用接收方的数字证书，对发送方的公钥进行加密生成数字信封，最后将数字信封和加密后的信息一起发送给接收方就可以实现信息安全。

数字信封保证了完整性，保密性。

解密过程如下：

1.先用私钥解密，得到发送方的对称密钥。

2.然后用对称密钥对加密后的信息进行解密，得到明文信息，消息摘要值和发送方的数字证书。利用摘要算法对

3.利用发送方数字证书中的密钥解密数字签名得到摘要

**第7章：HSAH函数（SHA-1的计算，弱碰撞强冲突的定义和区别）**

（1）HASH函数是公开的，它是单向加密函数

（2）6个要求：

1.任意输入

2.定长输出

3.计算迅速

4.单向计算，逆向困难

5.抗弱碰撞。即给定m和H（m）【它的hash值】，找到另一个不同的消息让他们hash值相等在计算上是不可能的。{条件是已知一条消息和其hash值。}

6.抗强冲突。让两个有意义的m和m1，让他们hash值相等在计算上是不可能的。{条件是已知两条消息。}

（3）SHA-1摘要值是160bits，其他的SHA后面杠几，摘要值就等于多少，比如SHA-384，摘要长度为384bits。

（4）每个分组是512bits，注意填充的计算。

（5）消息认证码的使用：MAC（message MACfunction code）:它只实现了完整性，不提供数字签名。其使用过程类似于hash的加解密，都是对码进行加解密，然后比较是否相等来保证完整性。

**第6章：公钥密码体制**

（1）基于大数分解问题的密码体制：RSA,Rabin

基于离散对数：Elgamal

基于椭圆曲线：SM2

（2）注意签名实现的过程，签名的计算，hash值比较的过程。

**第5章：序列密码体制（重点是线性反馈移位寄存器的计算，要注意通常会与第四章的分组密码的模式进行一起考核，因为会考核是否能作为密钥流生成器）**

（1）如果它的周期等于2的n次方-1，则此序列为m序列。N是它的级数，即有多少位。

（2）序列密码分为两种：同步序列密码和自同步序列密码。

区别是：

同步独立于消息产生，一旦失去同步（出错了），则必须停止发送所有消息，直到重新建立同步，才可以继续发送，接收方才可以接收到正确的密文分组。

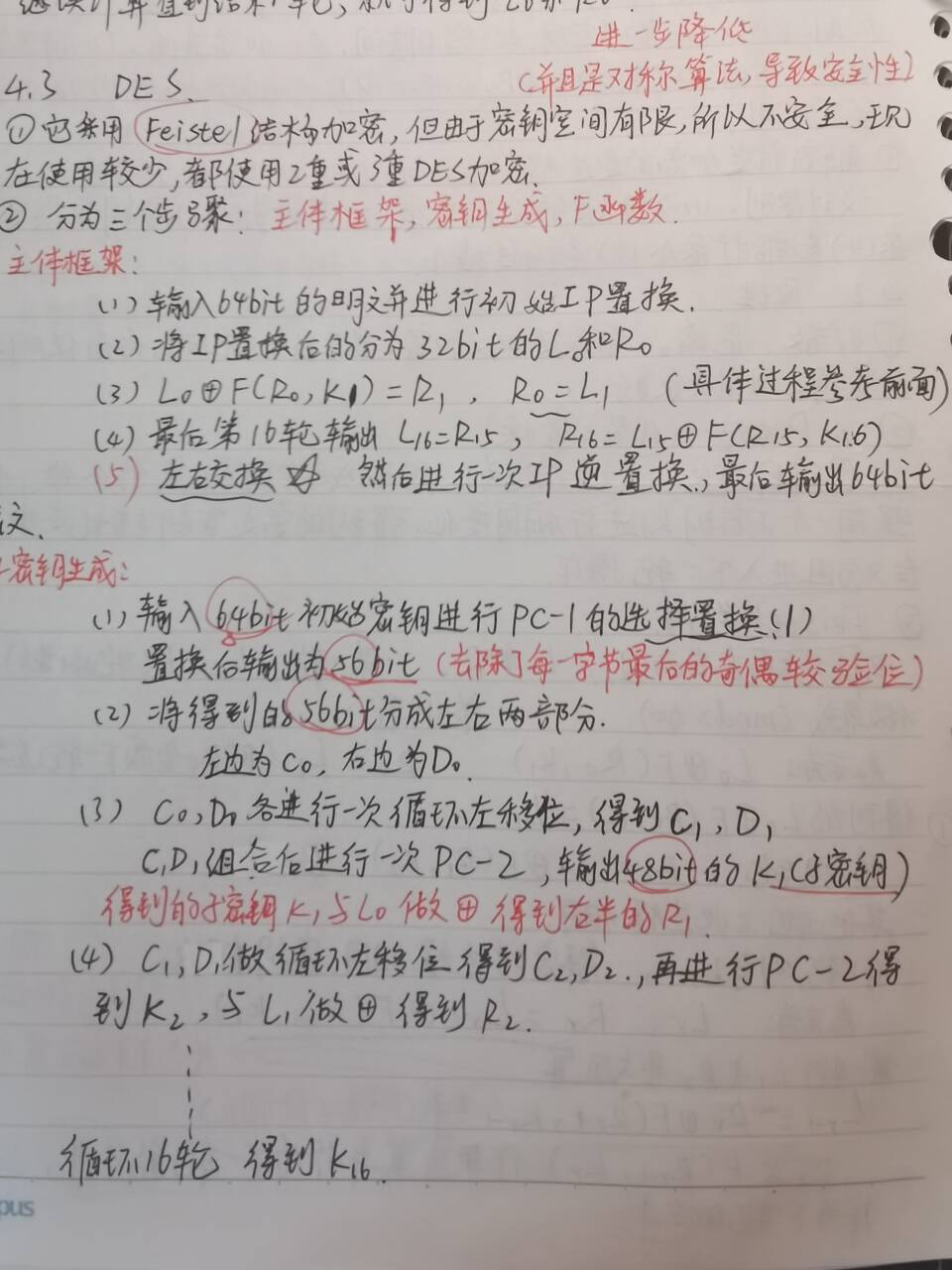
自同步与铭文分组有联系，如果出错了，只要接收到n（n是它的级数）个未出错的分组就可以自动重新建立同步。

同步：优点是无差错传播，容易检测主动攻击。缺点是一旦失去同步必须借助外部手段恢复典型代表有CTR

自同步：优点是不需要借助外部手段回复同步，容错率高，具有有限的差错传播。缺点是分析起来较为困难。典型代表有OFB,CFB

**第4章：分组密码体制（重点是算法DES，AES，5种密码体制及其特征）**

第一板块：DES，它是经典的feistel结构，AES不是



（2）需要注意的是有效密钥长度要将奇偶校验位去除，即一重des，有效密钥长度是56bits，3重为56\*3=162。

第二部分：AES

（1）有三种分组：明文128、192、256bits。密钥长度分别有：128、192、256分组。所以一共有3\*3=9种。

但是！！！！NIST选中的AES限定明文分组是128bits，所以根据密钥长度决定进行的轮数！！ 密钥长度对应的轮数为：128：10轮。192：12轮。256：14轮

（2）初始矩阵是按字节进行编排的，一个4\*4共计16字节的初始矩阵。

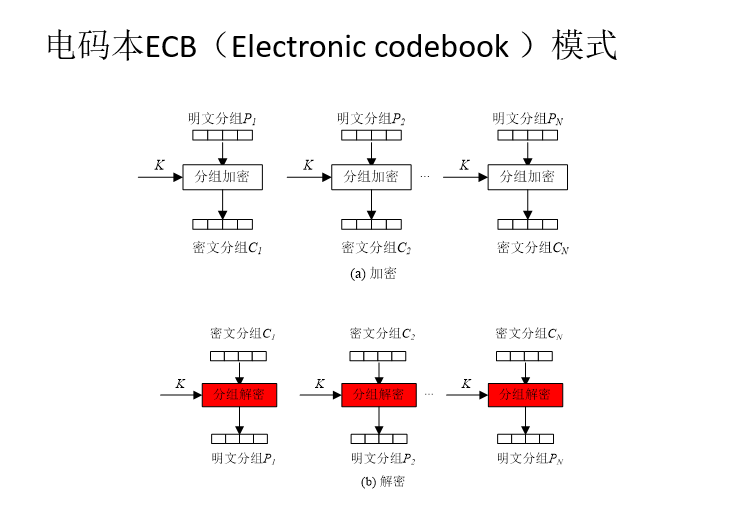
（3）过程是：明文块与子密钥做一次轮密钥加，然后（字节代替，行移位，列混合，轮密钥加）。进行完这些判断一次是否为最后一轮，若不是则循环进行括号中的部分，若是则进行最后的字节代替、行移位、列混合、轮密钥加得到密文块

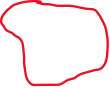
（4）初始密钥也是以字节为单位，组成一个6\*4的矩阵。以一列为一个单位。

第三部分：分组密码的工作模式ECB,CBC,CFB,OFB,CTR

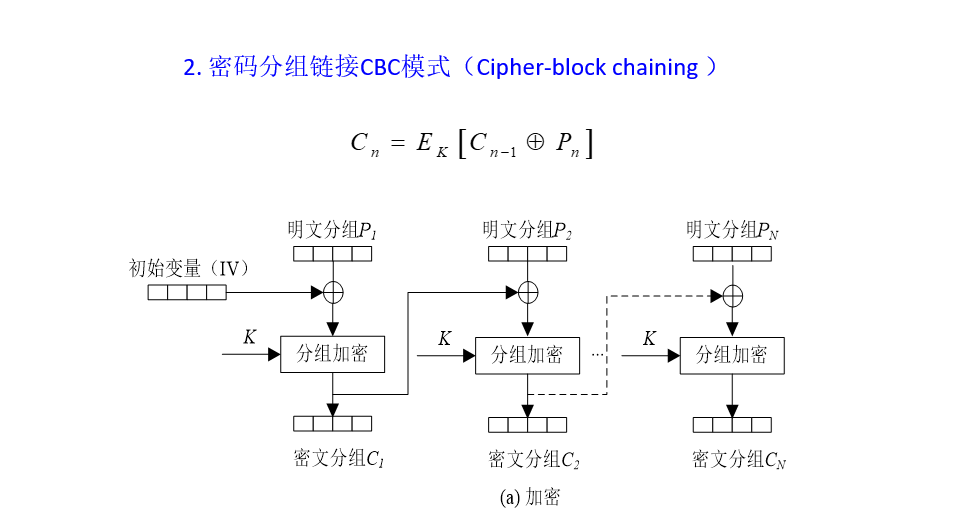
（1）有五种，如上

（2）ECB最简单，直接用铭文分组和轮密钥进行分组加密。无差错传播



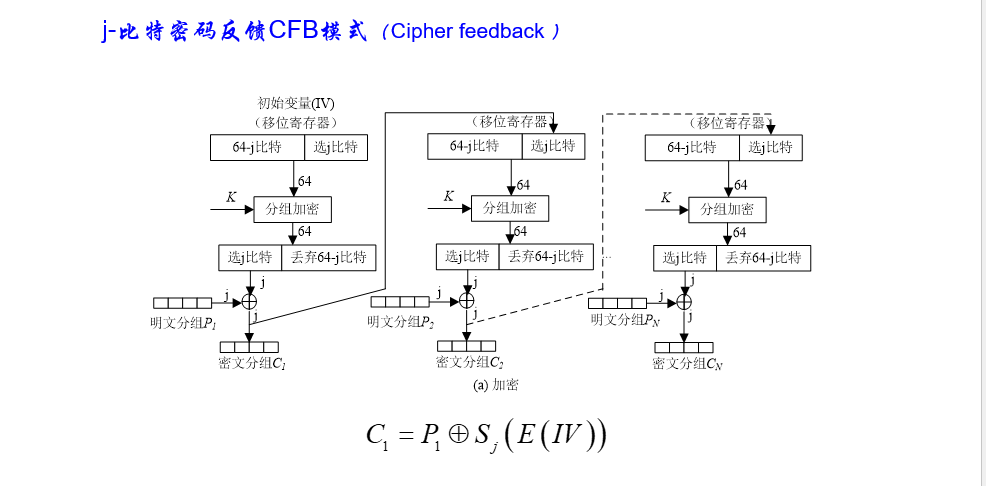


（3）CBC：思想是既然独立于明文不安全，那就将上一个分组的密文与下一个分组的明文产生联系，掩盖统计特性。



过程是：第一轮，明文先与初始变量做异或，然后与轮密钥进行分组加密得到密文分组。而第一轮得到的密文分组作为第二轮的初始变量与第二轮明文分组做异或，然后得到的在于第二轮的密钥进行分组加密，得到密文，第二组得到的密文作为第三轮的初始变量与第三组明文做异或。解密过程在ppt124页

特点：隐藏统计特性，bit错误时具有有限的差错传播、bit缺失时其后所有分组全错。

（4）CFB（cipher feedback，密文反馈）：要使用移位寄存器。过程如下：



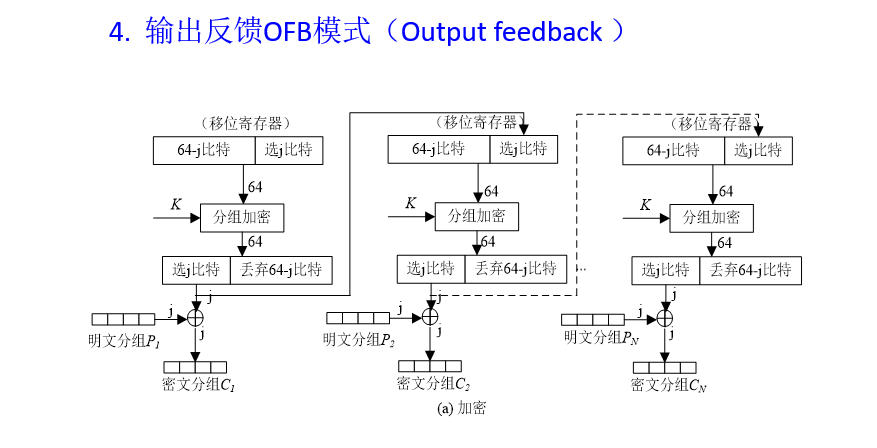
先对移位寄存器加密，输出64bits，然后选jbits与jbits的明文做异或，然后把密文jbits放到下一组的移位寄存器中。

特点：掩盖统计特性。若出现bits错误，会影响接下来许多个分组（直到那个错误的bit位移动出移位寄存器才会停止它的影响）。若出现bit缺失，则其后所有分组全错。

它可以作为同步密钥流生成器！！！！！

（5）OFB（output feedback，移位寄存器加密后的jbit输出反馈。）：

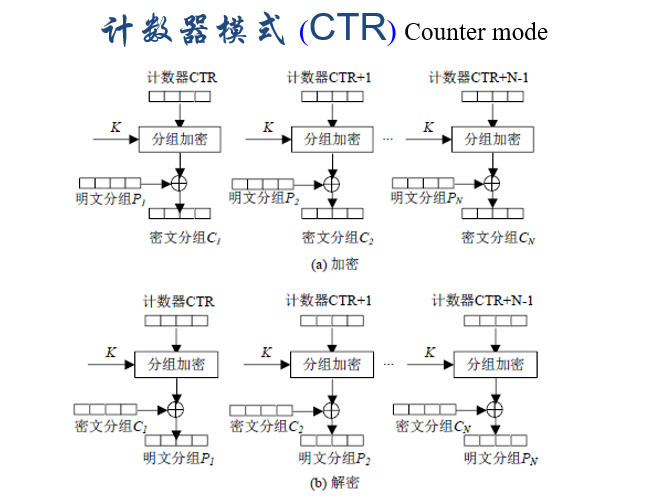
过程就是将CFB的密文进入下一组换成了寄存器输出进入下一组。





特性：无差错传播，掩盖了统计特性，可以作为自同步密钥流生成器。

（6）CTR模式：

先用密钥将计数器CTR加密，然后与明文做异或即可。

特点：无差错传播，掩盖了明文的统计特性。

**第3章：密码学相关算法**

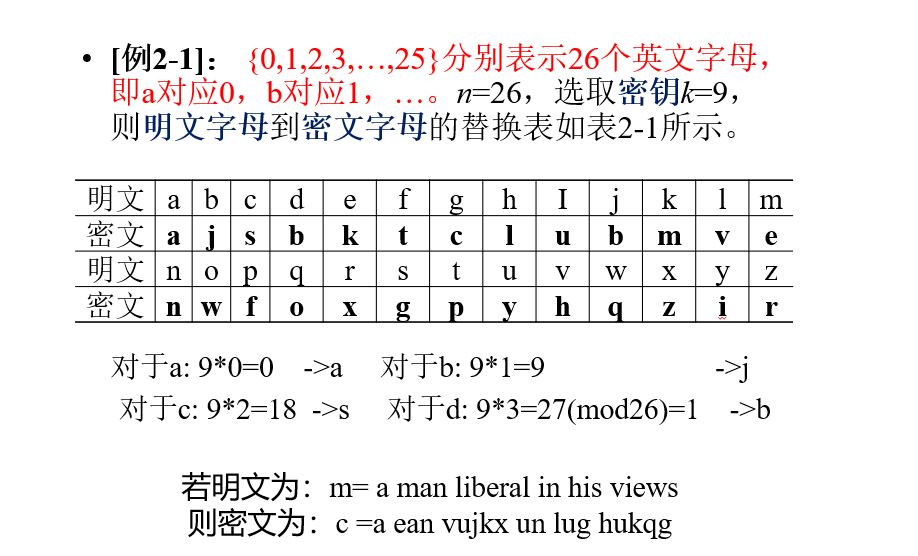
重点掌握：欧拉定理，模重复平方法，辗转相除法求逆元，扩展欧几里得算法。

**第2章：古典密码体制**

（1）主要分为两种：换位密码，代替密码。

（2）代替密码：分为单字符单表代换，单字符多表代换。

单字符单表的典型算法：乘法密码，加法密码，仿射密码。



统一从0开始编码，0-25，n=26，公式就是：c=m\*k mod26（乘法密码，

加法为m+k mod26）

多表代换密码：

维吉尼亚密码：给定一串密钥值，将明文分别按照密钥的偏移量向后移动进行代换。

弗纳姆算法（vernam），将明文和密文按位做异或（先转换成二进制）

古典密码分析：（1）加解密适用于所有密钥空间中的元素（2）系统便于实现和使用（3）达不到理论不可破，也应当实际不可破（4）安全性不能依赖于算法保密，而应该依赖于密钥保密。

第1章：密码学概论：

重点如下：