[第一讲：绪论](#3639-1609851323648)

[1.密码的含义及其主要功能](#7512-1609850849859)

[2.现代密码学与信息安全的关系](#6193-1609850849859)

[3.现代密码学的主要内容](#5114-1609850849859)

[第二讲：传统密码技术](#3593-1609850849859)

[1.密码学发展每个阶段的特点](#7171-1609850849859)

[2.现代密码学的两次飞跃及里程碑事件](#4653-1609850849859)

[3.学习传统密码技术的意义](#3667-1609850849859)

[4.转轮密码成功的启示](#8824-1609850849859)

[5.重合指数法](#0017-1609850849859)

[第三讲：密码学基本知识](#6584-1609850849859)

[1.密码系统的组成及它们之间的关系](#5623-1609850849859)

[2.现代密码体制的基本原则及公开算法的意义](#4183-1609850849859)

[3.密码体制的基本要求](#9859-1609850849859)

[4.密码的攻击类型及其含义](#9026-1609850849859)

[5.攻击密码体制的常用方法](#4444-1609852218427)

[6.算法复杂度的度量](#5256-1609850849859)

[第四、五讲：分组密码](#2859-1609850849859)

[1.分组密码的设计思想](#9219-1609850849859)

[2.分组密码的基本特点](#9041-1609850849859)

[3.互补性会使DES在选择明文攻击下所需的工作量减半](#8462-1609850849859)

[4.AES密码算法](#6960-1609858392209)

[5.二重DES并不像人们想象那样可提高密钥长度到112比特，而相当57比特](#9778-1609850849859)

[6.3DES的优点与不足](#5197-1609850849859)

[7.AES和DES各自组成、每部分的实现过程以及特点](#2830-1609850849859)

[8.AES和DES的相似与不同](#6631-1609850849859)

[9.分组密码五种操作模式各自特点（重点：ECB、CBC、CTR）](#5710-1609850849859)

[第七、八讲：公钥密码技术](#8968-1609850849860)

[1.公钥密码体制的优势与不足（与对称密码体制相比）](#2911-1609850849860)

[2.公钥密码算法应满足的要求是什么](#4682-1609850849860)

[3.RSA算法中，要求素数p和q的长度相差不能太大，大小相差比较大，是强素数，请说明原因](#1959-1609850849860)

[4.RSA算法的小结](#7798-1609850849860)

[5.针对ElGamal算法攻击的小步大步的基本思想](#3977-1609850849861)

[6.与RSA、Elgamal算法相比，ECC算法的优势](#5739-1609850849861)

[7.RSA、ElGamal、ECC算法的正确性证明](#9053-1609850849861)

[8.IBE算法的优势与不足](#8318-1609850849861)

[第九、十讲：hash函数及其应用](#3416-1609850849861)

[1.哈希函数的性质](#8310-1609850849861)

[2.哈希函数的安全性](#1415-1609850849861)

[3.消息认证码的作用](#4561-1609850849861)

[4.数字签名与手写签名的不同](#3053-1609850849861)

[5.数字签名算法的实现要求](#3017-1609850849861)

[6.在ElGamal签名算法中，如果使用相同的k对两个不同的消息进行签名，将会发生什么结果，为什么？](#2376-1609850849861)

[7.针对基于离散对数签名算法能够验证正确性，给出其计算量以及签名长度](#9900-1609850849861)

[第十一、十二讲：密钥管理技术](#7498-1609850849861)

[1.密钥管理遵循的原则](#8731-1609850849861)

[2.密钥的生命周期包含哪些阶段及其特点](#2463-1609850849861)

[（1）生成：](#5123-1609850849861)

[（2）存储：](#5057-1609850849861)

[（3）建立（分配和协商）](#8854-1609850849861)

[（4）使用：](#1912-1609850849861)

[（5）备份/恢复：](#6440-1609850849861)

[（6）更新：](#3019-1609850849861)

[（7）撤销/存档/销毁：](#6811-1609850849861)

[3.公钥证书包含哪些内容](#9020-1609850849861)

[4.数字证书验证包括哪些步骤](#8014-1609850871541)

[5.基于KDC的密钥分配方案](#9145-1609850849861)

[6.Diffie-Hellman密钥交换方案](#4425-1609850849861)

[7.举例说明文件加密传送方案](#1128-1609850849861)

[8.Shamir门限方案](#3440-1609850849861)

**第一讲：绪论**

**1.密码的含义及其主要功能**

含义：密码学是一个非常庞大而复杂的信息处理系统，涉及信息的机密性、完整性、认证性、不可否认性等许多方面，属于信息安全范畴。

主要功能：

机密性：是指保证信息不被泄露给非授权的用户或实体，确保存储的信息和传输的信息仅能被授权的各方得到，而非授权用户及时得到信息也无法知晓信息内容，不能使用。

完整性：是指信息未经授权不能进行改变的特征，维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改（插入、替换、删除、重排序等），如果发生，能够及时发现。

认证性：是指确保一个信息的来源或源本身被正确地标识，同时确保该标识的真实性，分为实体认证和消息认证。（实体认证：参与信息处理的实体是可信的，即每个实体的确是它所宣称的那个实体，使得任何其它实体不能假冒这个实体。消息认证：能够向接收方保证该信息确实来自于它所宣称的源。）

不可否认性：是防止发送方或接收方抵赖所传输的信息，要求无论发送方还是接收方都不能抵赖所进行的行为。因此，当发送方发送一个信息时，接收方能证实该信息的确是由所宣称的发送方发来的；当接收方收到一个信息时，发送方能够证实该信息的确送到了指定的接收方。

**2.现代密码学与信息安全的关系**

密码学是与信息安全多方面有关的数学技术的研究。

密码学是保证信息安全的核心技术，但不是提供信息安全的唯一方式。

信息安全是密码学研究与发展的目的。

信息安全的理论基础是密码学，信息安全的问题根本解决通常依靠密码学理论。

**3.现代密码学的主要内容**

**第二讲：传统密码技术**

**1.密码学发展每个阶段的特点**

古典密码时期：从古代到19世纪末，长达几千年。技术工具：手工。通信手段：信使。密码体制：纸、笔或者简单器械实现的代换及置换，是一种艺术。典型密码：凯撒密码、维吉尼亚密码。

近代密码时期：从20世纪初到20世纪50年代，即一战二战时期。技术工具：机械设备。通信手段：电报。密码体制：手工或电动机械实现复杂的代换及置换，仍是一门艺术。典型密码：Vernam密码、转轮密码。

现代密码时期：从20世纪50年代至今。技术工具：计算机。通信手段：无线通信、有线通信、计算网络等。密码体制：分组密码、序列密码以及公钥密码，有坚实的数学理论基础，成为一门科学。典型密码：DES、AES、RC4、RSA、ECC、SHA。

**2.现代密码学的两次飞跃及里程碑事件**

第一次飞跃：1949年香农发表题为《保密系统的通信理论》，为密码系统建立了理论基础，从此密码学成为了一门科学。

里程碑事件：1976年后，美国数据加密标准（DES）的公布使密码学的研究公开，密码学得到了迅速发展。

第二次飞跃：1976年，Diffe和Hellman发表了《密码学的新方向》，提出了一种新的密码设计思想，从而开创了公钥密码学的新纪元。

里程碑事件：1978年由Rivest、Shamire、Adleman首先提出第一个实用的公钥密码体制RSA，使公钥密码的研究进入了快速发展阶段。

**3.学习传统密码技术的意义**

传统密码体制的技术、思想以及分析方法虽然很简单，但是反映了密码设计和分析的思想，是学习密码学的基本入口，对于理解、设计和分析现代密码仍然具有借鉴的价值。

**4.转轮密码成功的启示**

转轮密码机是近代密码发展史中的里程碑事件。

启示：使用密码设备应必备四要素：安全、性能、成本、易用

**5.重合指数法**

具体可以看课件，关键：两个不同的英文文本找到两个等同字母的概率为0.065

**第三讲：密码学基本知识**

**1.密码系统的组成及它们之间的关系**

一个密码系统是由明文、密文、加密算法和解密算法、密钥五个部分组成的。

信息的原始形式称为明文。

明文经过编码变换所生成的称为密文。

对明文进行编码变换生成密文的过程称为加密，编码的规则称为加密算法。

将密文恢复出明文的过程称为解密，恢复的规则称为解密算法。

密钥控制明文与密文之间的相互变换，分为加密密钥和解密密钥。

**2.现代密码体制的基本原则及公开算法的意义**

Kerckhoffs原则：密码系统中的算法即使为密码分析者所知，也无助于用来推导出明文或密钥。也就是说，密码系统的安全性不应取决于不易改变的密码算法（公开、标准化），而应取决于可随时改变的密钥。

意义：有利于增强密码算法的安全性；有利于密码技术的推广应用；有利于增加用户使用的信心；有利于密码技术的发展。

**3.密码体制的基本要求**

密码体制的安全性依赖密钥的安全性，密码算法是公开的。

密码算法安全强度高，也就是说，密码分析者除了穷举搜索攻击外再找不到更好的攻击方法。

密钥空间应足够大，使得试图通过穷举密钥空间进行搜索的方式在计算上不可行。

加密函数和解密函数都可以高效地满足实际需求。

密码体制既易于实现又便于使用。

**4.密码的攻击类型及其含义**

惟密文攻击：密码分析者除了拥有截获的密文外，没有其它可以利用的信息。这种情况下进行密码破译是最困难的，经不起这种攻击的密码体制被认为是完全不安全的。

已知明文攻击：密码分析者不仅掌握了相当数量的密文，还有一些已知的明-密文对可供利用。对于现代密码体制的基本要求，不仅要经受得住惟密文攻击，而且要经受得住已知明文攻击。

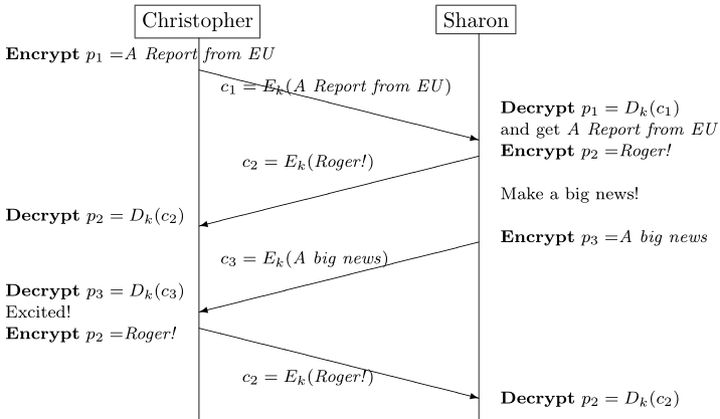
选择明文攻击：密码分析者不及能够获得一定数量的明-密文对，还可以选择任何明文并在使用同一未知密钥的情况下能得到相应的密文。（暂时控制加密机）

选择密文攻击：密码分析者能选择不同被加密的密文，并还可得到对应的明文。（暂时控制解密机）

选择文本攻击：选择明文攻击和选择密文攻击的组合，即密码分析者在掌握密码算法的前提下，不仅能够选择明文并得到对应的密文，而且还能选择密文得到对应的明文。（暂时控制加密机和解密机）

抵御这五种类型的攻击是密码算法的基本要求。

这里我们首先假设通信双方，Sharon和Christopher已经完成了秘钥交换，秘钥k是双方已知的，开始进行如下通信：



那么通信过程中一共产生的消息是三组明密文对

，

和

**唯密文攻击**：只知道密文，也就是

，那只能通过统计特性分析其中有什么规律了

**已知明文攻击**：得到了一些给定的明文和对应的密文，在这里可以是

的任意非空子集。

**选择明文攻击**：除了上面的基础，攻击者还可以任意创造一条明文比如“Excited”，并得到其加密后的密文。比如用一定的手段渗透Sharon的系统，但是不能直接攻破秘钥，于是只能以她的身份发“Excited”，然后用抓包或者别的方法得到她发送出来的加密的消息。

**选择密文攻击**：除了已知明文攻击的基础，攻击者还可以任意制造或者选择一些密文，并得到其解密后的明文。比如用一定的手段在通信过程中伪造消息替换真实消息，然后窃取Sharon获得并解密的结果，有可能正好发现随手伪造的密文解密结果是有意义的，比如naive。

**选择文本攻击**：可以制造任意明文/密文并得到对应的密文/明文，就是上面两者的结合。

**5.攻击密码体制的常用方法**

（1）穷举攻击：密码分析者试编所有密钥的方法来破译密码。

对抗穷举攻击：

增大密钥量，当密钥量增大时，尝试的次数必然增大。（最好方法）

加大算法复杂性，当算法的复杂性增大，完成一次加/解密所需的时间也增大，从而使穷举攻击的时间也增加，但这也增加了合法用户使用密码系统的计算量。

（2）统计分析攻击：密码分析者通过分析密文和明文的统计规律来破译密码。大多数传统密码都可以通过统计分析的方法来破译。

对抗统计分析攻击：设法使明文的统计特征尽可能地不带入密文，如果密文不带有明文的痕迹，统计分析攻击成为不可能。

（3）数学分析攻击：密码分析者针对加密变换所依赖的数学难题（大整数的素因子分解、离散对数等），通过数学求解的方法（二次筛法、积分指数法等）来设法找到相应的解密变化，从而实现破译。

对抗数学分析攻击：选用具有坚实的数学基础和足够复杂的加密方法。

**6.算法复杂度的度量**

算法的计算复杂性由它所需的时间和空间量级来度量，其优点是独立于所用的系统并且使人们看到时间和空间的需求随输入的规模n而增长。通常按时间复杂性对算法进行分类。密码设计者希望对密码的任何攻击算法都具有指数级的时间复杂度，这样对密码的攻击实际上都是计算上不可行的。

**第四、五讲：分组密码**

**1.分组密码的设计思想**

分组密码的设计思想包括扩散和混乱。

（1）扩散：扩散是指要将算法设计成明文每一比特的变化尽可能多地影响到输出密文序列的变化，以便隐藏明文的统计特性。（雪崩效应）扩散的目的是希望密文中的任意比特都要尽可能与明文、密钥相关联，或者说，明文和密钥中的任意比特值发生改变，都会在某种程度上影响到密文值的变化，以防止将明文或密钥分解成若干个孤立的小部分，然后被各个击破。

（2）混乱：混乱是指在加解密变换过程中明文、密钥以及密文之间的关系尽可能地复杂化，以防密码破译者采用解析法进行破译攻击。混乱应是可逆的，即明文混乱后能得到密文，密文经过逆向混乱操作能恢复出明文。按照混乱原则，分组密码算法应有复杂的非线性因素。

**2.分组密码的基本特点**

（1）分组长度：能够抵御选择明文攻击

（2）密钥长度：能够抵御穷举攻击

（3）子密钥：子密钥的生成是迭代分组算法的一个重要组成部分，是从初始密钥产生各轮迭代要使用的子密钥的算法。

子密钥的评价指标：

实现简单、快速，满足轮函数F的要求

初始密钥的所有比特对每个子密钥比特的影响应大致相同

没有弱密钥或者弱密钥容易确定

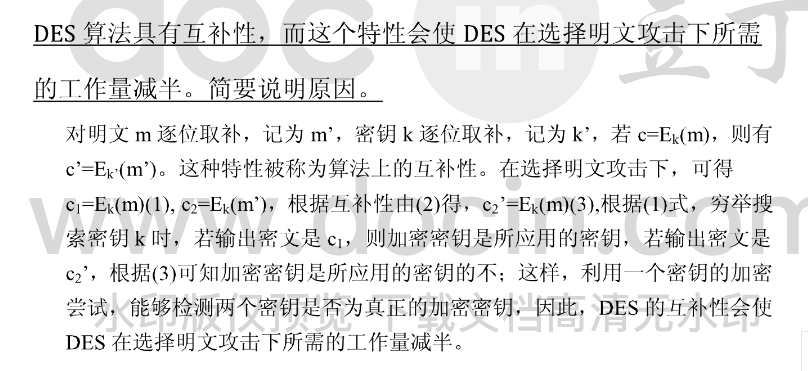
（4）轮函数F：分组密码的核心，是分组密码中单轮加解密函数，基本准则：非线性（依赖S盒）、可逆性、雪崩效应。主要性能指标：安全性、速度、灵活性。

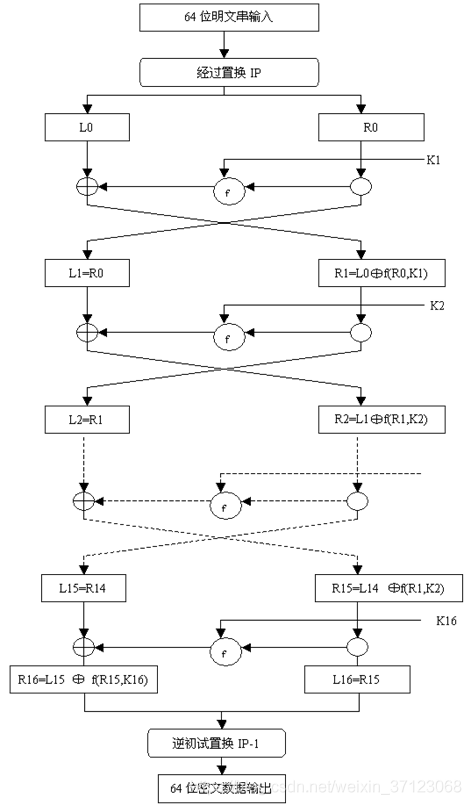
（5）迭代：分组密码一般采用简单的、安全性若的密码函数进行多轮迭代运算，使得安全性增强。一般来说，分组密码迭代轮数越多，密码分析越困难，但过多的迭代轮数会使加解密算法的性能下降，而实际的安全性增强不明显。

决定迭代轮数的准则：密码算法分析的难度大于简单穷举搜索攻击的难度。

**3.互补性会使DES在选择明文攻击下所需的工作量减半**

<https://www.bilibili.com/video/BV1QW411B7A4?from=search&seid=9426716109116003429>





**4.AES密码算法**

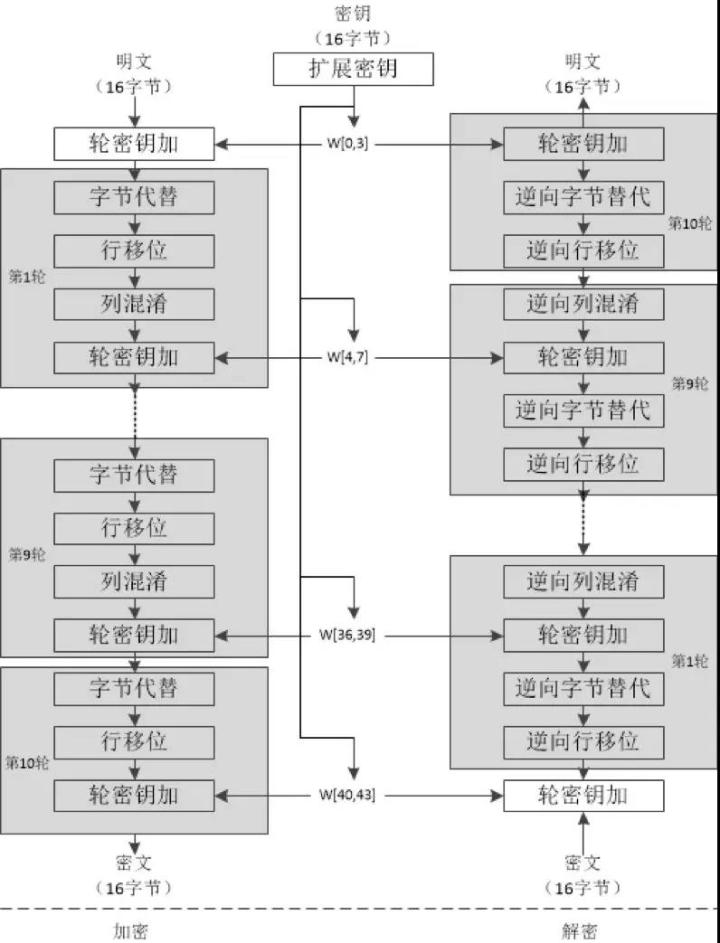
算法的开始和结束阶段都要使用轮密钥加，且仅仅在该阶段使用密钥

每轮由四个阶段构成：字节代换、行位移、列混淆、轮密钥加（异或）

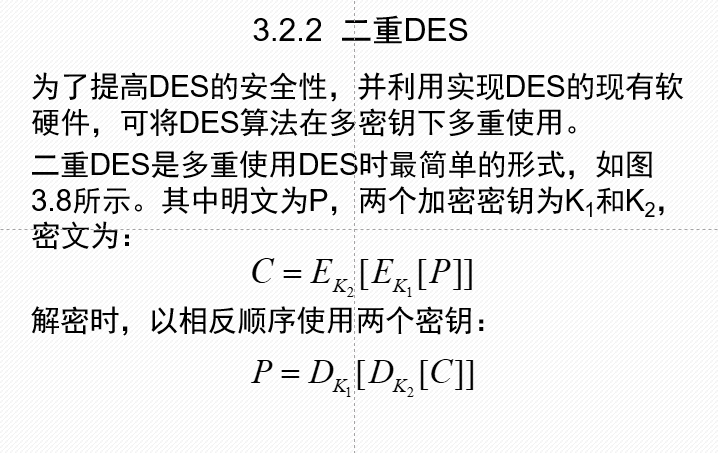
每个阶段均可逆，加解密算法不相同

最后一轮只包含三个操作：字节代换、行位移、轮密钥加

<https://www.sohu.com/a/201169795_466846>



**5.二重DES并不像人们想象那样可提高密钥长度到112比特，而相当57比特**



**6.3DES的优点与不足**

优点

密钥长度增加到112位或168位，克服了DES面临的穷举攻击。

相对于DES，增强了抗差分分析和线性分析等的能力。

由于DES已经大规模使用，升级到3DES比更新新算法成本小得多。

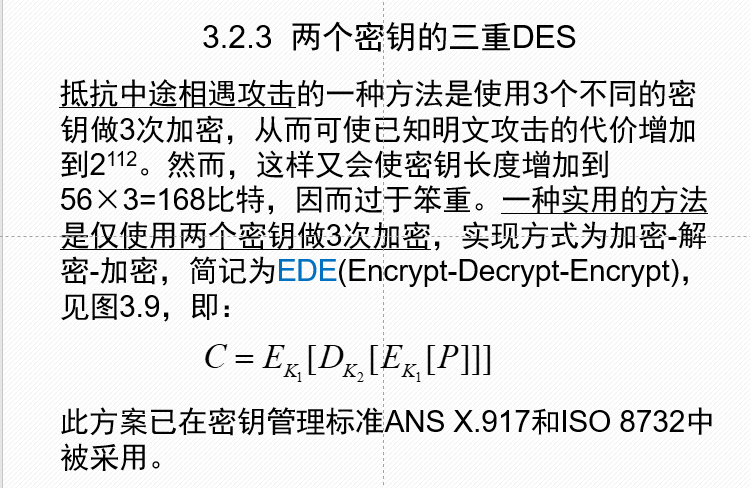
DES比其它任何加密算法受到的分析时间都长的多，相应地，3DES抗分析能力更强。

不足：

3DES处理速度较慢

虽然密钥长度增加了，但明文分组长度没变，与密钥长度的增常不匹配。

3DES是DES向AES过度的加密算法。



**7.AES和DES各自组成、每部分的实现过程以及特点**

结合流程图记忆效果更佳。

**8.AES和DES的相似与不同**

相似：

（1）二者的轮函数都是由四层构成，非线性层、移位层、线性混合层、子密钥异或，只是顺序不同。

（2）AES的非线性运算是字节代替，对应于DES中的非线性运算S盒。

（3）行移位运算保证了每一行的字节不仅仅影响其它行对应的字节，而且影响其它行所有的字节，这与DES中置换P相似。

（4）AES的列混淆运算的目的是让不同的字节相互影响，而DES中F函数的输出与左边一半数据相加也有类似的效果。

（5）AES的子密钥异或对应于DES中S盒之前的子密钥异或。

不同：

（1）AES的密钥长度（128位、192位、256位）是可变的，而DES的密钥长度固定为56位。

（2）DES是面向比特的运算，AES是面向字节的运算

（3）AES的加密运算和解密运算不一致，因而加密器不能同时作为解密器，而DES的加器可用作解密器，只是子密钥的顺序不同。

**9.分组密码五种操作模式各自特点（重点：ECB、CBC、CTR）**

<https://blog.csdn.net/weixin_42940826/article/details/83687007>

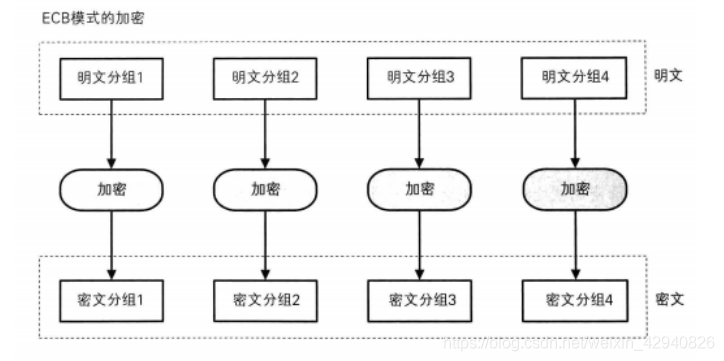
（1）电子密码本模式（ECB）：

模式操作简单，主要用于内容较短且随机的报文的加密传递

相同明文（在相同密钥下）得出相同的密文，即明文中的重复内容可能将在密文中表现出来，易实现统计分析攻击、分组重放攻击和代换攻击。

链接依赖性：各组的加密都独立于其它分组，可实现并行处理。

错误传播：单个密文分组中有一个或多个比特错误只会影响该分组的解密结果



（2）密码分组链接模式（CBC）：

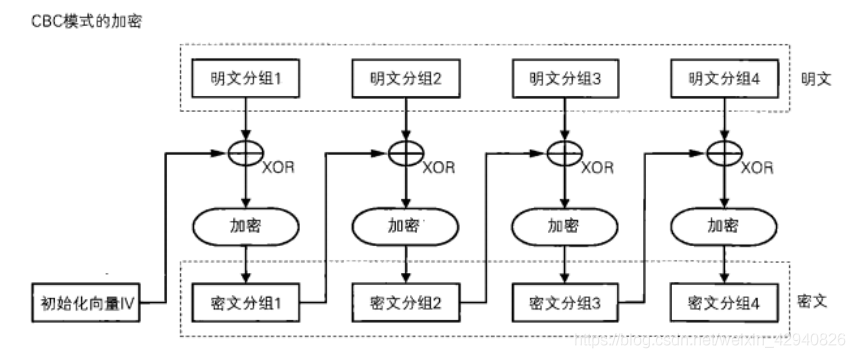
一种反馈机制在分组密码中的应用，每个密文分组不仅依赖于产生它的明文分组，还依赖于它前面的所有分组

相同的明文，即使相同的密钥喜爱也会得到不同的密文分组，隐藏了明文的统计特性

链接依赖性：对于一个正确密文分组的正确解密要求它之前的那个密文分组也正确，不能实现并行处理

错误传播：密文分组中的一个分组出现错误会影响到本组和其后分组的解密，错误传播为两组

初始化向量IV不需要保密，它可以以明文形式与密文一起传送。



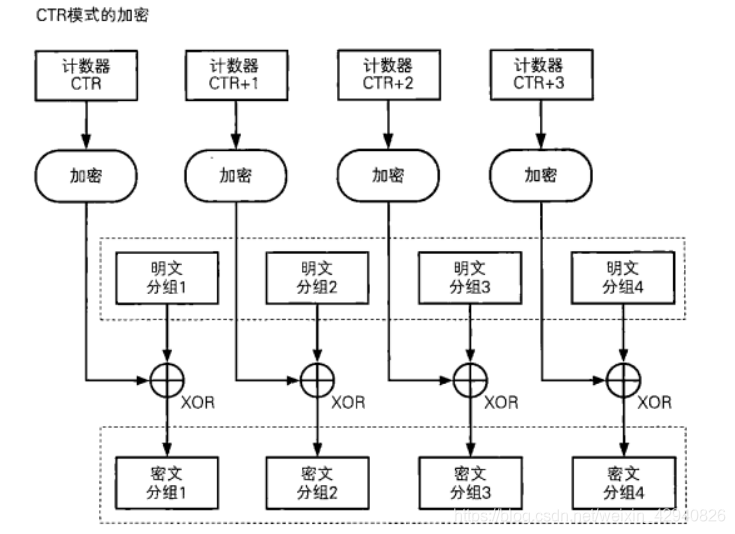
（3）计数器模式（CTR）：

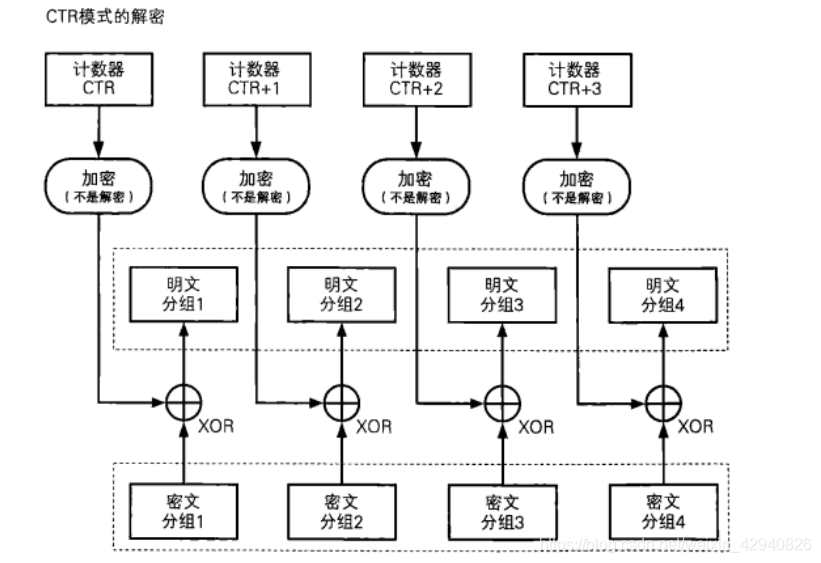
效率高：能够并行处理多块明（密）文，可用来提供像流水线、每个时钟周期的多指令分派等并行操作

预处理：基本加密算法的执行并不依赖明文或密文的输入，可预先处理，当给出明文或密文时，所需的计算仅是进行一系列的异或运算

随机访问：密文的第i个明文组能够用一种随机访问的方式处理

简单性：只要求实现加密算法而不要求实现解密算法，像AES这类加解密算法不同就更能体现CTR的简单性。





（4）密文反馈模式（CFB）：

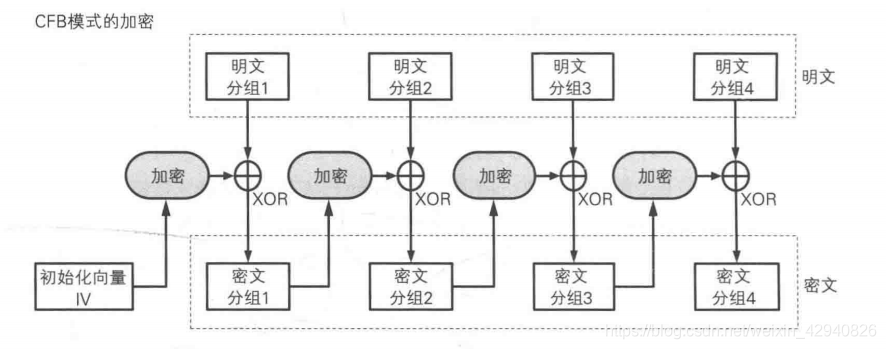
消息被看作数据分组流，不需要整个数据接收完后才能进行加解密

可用于自同步序列密码

具有CBC模式的优点

对新到错误较敏感且会造成错误传播

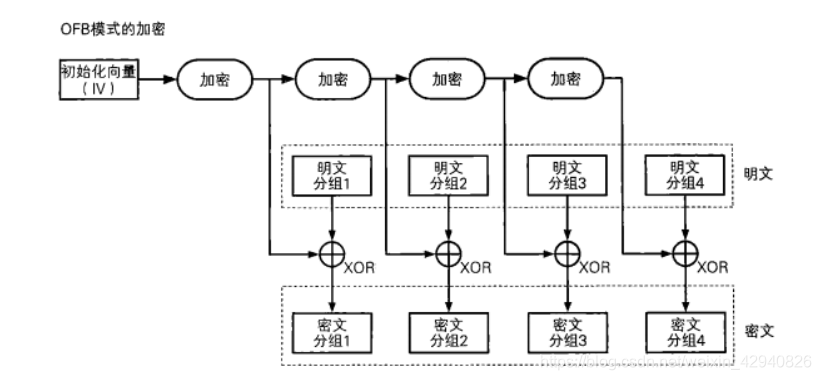
数据加解密的速率降低，其数据率不会太高



（5）输出反馈模式（OFB）：

OFB模式是CFB模式的一种变形，克服由错误传播带来的问题，但对密文被篡改难于进行检测

OFB模式不具有自同步能力，要求系统保持严格的同步，否则难于解密



ECB是最快、最简单的分组密码模式，但它的安全性最弱，一般不推荐使用ECB加密消息，但如果是加密随机数据，如密钥，ECB则是最好的选择。

CBC适合文件加密，而且又少量错误时不会造成同步失败，是软件加密的最好选择。

CTR结合ECB和CBC的优点，最近为人们所重视，在ATM网络和IPSec中起了重要作用。

**第七、八讲：公钥密码技术**

**1.公钥密码体制的优势与不足（与对称密码体制相比）**

优势：

（1）密钥分发简单

（2）需秘密保存的密钥量减少

（3）可以实现数字签名和认证的功能

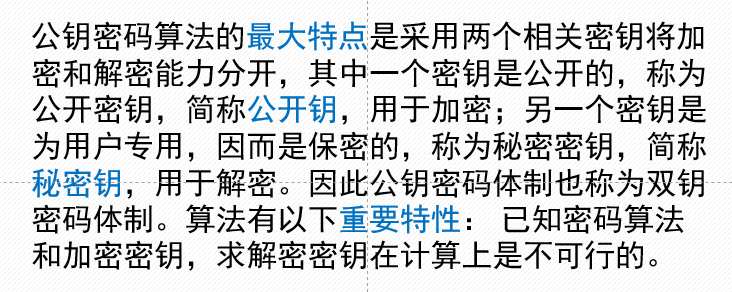
不足：

（1）比对称密码算法慢

（2）公钥密码算法提供更多的信息对算法进行攻击，如公钥密码算法对选择明文攻击是脆弱的，尤其明文集比较小的时候

（3）有数据扩展

（4）公钥密码算法一般是建立在对一个特定的数学难题的求解上，往往这种困难性只是一种设想。



**2.公钥密码算法应满足的要求是什么**

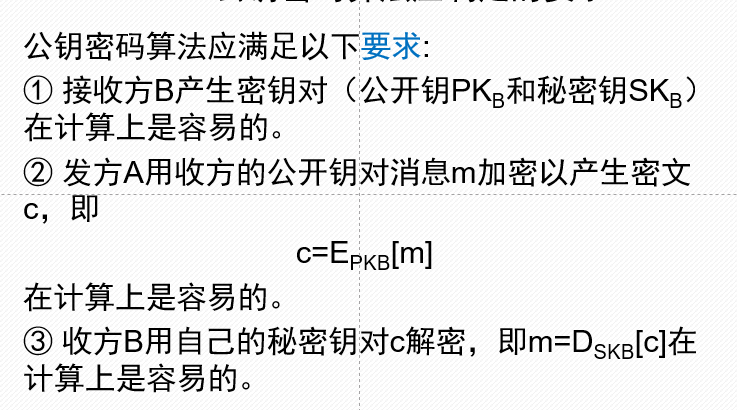
（1）密钥对的产生在计算上是容易的

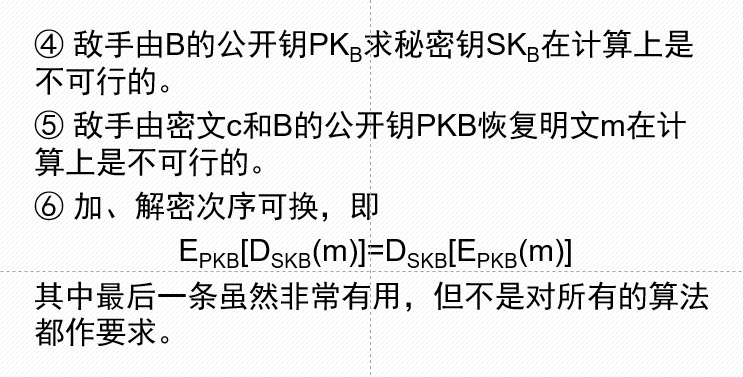
（2）利用公钥对消息m加密以产生密文c在计算上是容易的

（3）利用私钥大于密文c解密在计算上是容易的

（4）攻击方由公钥求私钥在计算上是不可行的

（5）攻击方由密文和公钥恢复明文或求私钥在计算上是不可行的





**3.RSA算法中，要求素数p和q的长度相差不能太大，大小相差比较大，是强素数，请说明原因**

长度不能相差太大：抵御试除法的攻击

强素数：p-1和q-1都应有大的素数因子，以抵御循环攻击

**4.RSA算法的小结**

第一个实用的公开密钥算法

目前使用最多的一种公钥密码算法

RSA的理论基础是数论的欧拉定理

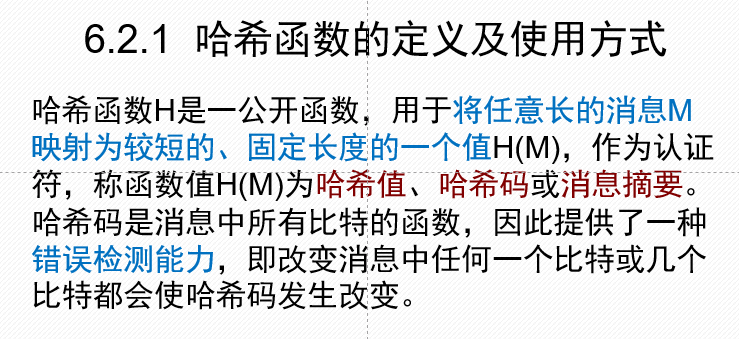
RSA的安全性依赖于大数的素因子分解的困难性

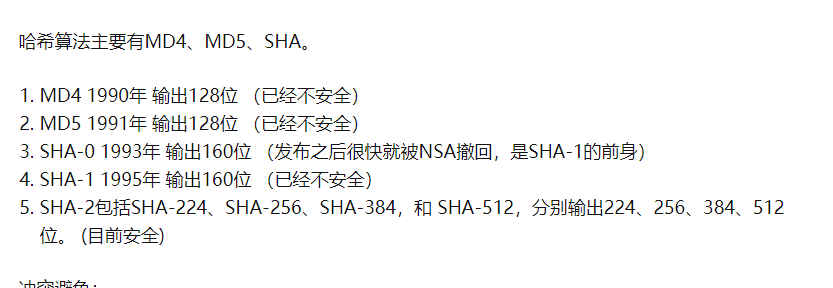
密码分析者既不能证明也不能否定RSA的安全性

既能用于加密也能用于数字签名

目前密钥长度1024位是安全的

**第九、十讲：hash函数及其应用**





**1.哈希函数的性质**

输入：消息是任意有限长度

输出：哈希值时固定长度

容易计算：对于任意给定的消息，容易计算出其哈希值（正向容易）

单向性：对于给定的哈希值h，要找到M使得H(M)=h在计算上是不可行的。（逆向不可行）

**2.哈希函数的安全性**

抗弱碰撞性：对于给定的消息M1，要发现另一个消息M2，满足H(M1)=H(M2)在计算上是不可行的。

抗强碰撞性：找任意一对不同的消息M1, M2，使H(M1)=H(M2)在计算上是不可行的。

随机性：当一个输入位发生变化时，输出位将发生很大的变化。（雪崩效应）

**3.消息认证码的作用**

接收方能够相信发送发发来的消息未被篡改。这是因为攻击者不知道密钥，所以不能够在篡改消息后相应地篡改MAC，而如果仅篡改消息，则接收方计算的新MAC将与收到的MAC一定是不同的。

接收方相信发送方不是冒充的。这是因为除收发双方外再无其他人知道密钥，因此其他人不可能对发送方发送的消息计算出正确的MAC。

**4.数字签名与手写签名的不同**

签名：手写签名是被签文件的物理组成部分；数字签名是连接到被签消息上的数字串。

传输方式：数字签名和所签名的消息能够在通信网络中传输；手写签名使用传统的安全方式传输。

验证：手写签名是通过将它与真实的签名进行比较来验证；而数字签名是利用已经公开的验证算法来验证。

数字签名的复制是有效的；而手写签名的复制品是无效的。

手写签名是模拟的，且因人而异；数字签名是0和1的数字串，因消息而异。

**5.数字签名算法的实现要求**

签名的产生必须使用签名者独有的一些信息（私钥）以防伪造和否认，同时，要求保证独有的一些信息的安全性。

签名的产生应较为容易。

签名的识别和验证应较为容易。

对已知的数字签名构造以新消息的数字签名在计算上是不可行的。（Hash的安全）

对已知消息构造以假冒的数字签名在计算上是不可行的。（私钥的安全）

**6.在ElGamal签名算法中，如果使用相同的k对两个不同的消息进行签名，将会发生什么结果，为什么？**

不能泄露随机数k。

不能使用相同的k对两个不认同消息进行签名。

【一旦得到k，很容易计算出签名者的私钥】

**7.针对基于离散对数签名算法能够验证正确性，给出其计算量以及签名长度**

**第十一、十二讲：密钥管理技术**

**1.密钥管理遵循的原则**

明确密钥管理的策略和机制：策略是密钥管理系统的高级指导，而机制是实现和执行策略的技术机构和方法。

（1）全面安全原则：必须对密钥生命周期的各个阶段采取妥善的安全管理。

（2）最小权利原则：只分配给用户进行事务处理所需的最小密钥集合。

（3）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种功能。

（4）密钥分级原则：对于一个大的系统，所需要的密钥的种类和数量都很多，根据密钥的职责和重要性，把密钥划分为几个级别。

（5）密钥更换原则：密钥必须按时更换。否则，即使采用很强的密码算法，只要攻击者截获足够多的密文，密钥被破译的可能性就非常大。

（6）密钥应有足够的长度：密钥安全的一个必要条件是密钥有足够的长度。

（7）密钥体质不同，密钥管理也不同：由于传统密码体制与公开密码体制是性质不同的两种密码，因此它们在管理方面有很大的不同。

**2.密钥的生命周期包含哪些阶段及其特点**

**（1）生成：**

密钥的长度与产生机制直接影响密码系统的安全，对于一个密码系统，如何产生好的密钥是很关键的，密钥生成是密钥生命周期的基础阶段。

密钥的生成一般首先通过密钥生成器借助于某种随机源产生具有较好统计分析特性的序列，以保障生成密钥的随机性和不可预测性，然后再对这些序列进行各种随机性检验以确保其具有较好的密码特性。

用户可以自己生成所需的密钥，也可以从可信中心或密钥管理中心申请，密钥长度要适中，至少能够抵御穷举攻击。

不同的密码体制或密钥类型，其密钥的具体生成方法一般是不相同的，与相应的密码体制或标准相联系。

**（2）存储：**

密钥的安全存储实际上是针对静态密钥的保护。其目的是确保密钥的秘密性、真实性以及完整性。

**（3）建立（分配和协商）**

**（4）使用：**

利用密钥进行正常的密码操作，如加密/解密、签名/验证等，通常情况下，密钥在有效期之内授权的用户都可以使用。

应注意使用环境对密钥安全性的影响。

密钥安全使用的原则是不允许密钥以明文的形式出现在密钥设备之外。通常使用智能设备来实现，但成本高，性能低。

**（5）备份/恢复：**

指密钥处于使用状态时的短期存储，为密钥的恢复提供密钥源。要求安全方式存储密钥，并且具有不低于正在使用的密钥的安全控制水平，不同的密钥，其备份的手段和方式差别较大。

如果密钥过了使用有效期，密钥将进入存档阶段或销毁阶段。

当密钥因为认为的操作错误或设备发生故障时可能发生丢失和损坏，因此任何一种密码设备应当具有密钥恢复的措施。从备份或存档中获取密钥的过程称为密钥恢复。若密钥丧失但其安全未受威胁，就可以用安全方式从密钥备份中恢复。

密钥恢复措施需要考虑恢复密钥的效率问题，能在故障发生后及时恢复密钥。

**（6）更新：**

以下情况需要更新：密钥有效期结束；密钥的安全受到威胁；通信成员中提出更新密钥。

更新密钥应不影响信息系统的正常使用，密钥注入必须在安全环境下进行并避免外漏。现用密钥和新密钥同时存在时应处于同等的安全保护水平下。更换下来的密钥一般情况下应避免再次使用，除将用于归档的密钥及时采取有效的保护措施以外应及时进行销毁处理。

更新方法：

利用密钥建立协议，重新生成新的密钥

利用已有的密钥，产生新的密钥

好处：效率高

安全要求：新密钥泄漏不设计已有密钥的安全

**（7）撤销/存档/销毁：**

撤销：若在密钥使用中密钥的安全受到威胁或提前中止，需要将它从正常使用的集合中删除，密钥将进入存档阶段或销毁阶段。

存档：当密钥不再使用且在有效期内时，需要对其进行存档，以便在某种特别需要情况下能够对其进行检索并使用。存档的密钥是离线保存的，处于使用后状态。

销毁：如果密钥过了有效期，即处于过期状态，将清除密钥及与该密钥相关的痕迹。

**3.公钥证书包含哪些内容**

版本号：用来区分X.509的不同版本

序列号：由发证机构给予每一个证书的分配唯一的数字型编号

认证机构标识：发证机构的名称

主体标识：证书持有者的名称

主体公钥：与该主体私钥相对应的公钥

证书有效期：包括两个日期，证书开始有效期和证书失效期

证书用途：描述该主体的公/私钥对的合法用途

扩展内容：说明该证书的附加信息

发证机构签名：用发证机构私钥生成的数字签名

**4.数字证书验证包括哪些步骤**

使用CA证书验证终端实体证书有效性

检查证书的有效期，确保该证书是否有效

检查该证书的预期用途是否符合CA在该证书中制定的所有策略限制

在证书撤销列表（CRL）中查询确认该证书是否被CA撤销。

**5.基于KDC的密钥分配方案**

建立一个负责为用户分配密钥的密钥分配中心，这时每一用户必须和密钥分配中心有一个共享密钥，称为主密钥。通过主密钥分配给一对用户的密钥称为会话密钥，用于这一对用户之间的保密通信。通信完成后，会话密钥即被销毁。如果用户数为n，则会话密钥数为n(n-1)/2，但主密钥数却只需n个。

**6.Diffie-Hellman密钥交换方案**

**7.举例说明文件加密传送方案**

**8.Shamir门限方案**