**一、题目类型 2017年考题**

概念题：计算安全、网络安全模型、ECB、一次一密、穷举攻击、雪崩效应、IPSec/VPN、Feistel加密结构特征、MAC函数、DH协议。

大题。

1.公钥体系、对称加密体系、MAC、HASH、数字签名在认证上的作用、特点。

2.凯撒密码与现代密码区别，如何改进成为现代密码。

3.防止重放攻击方法。

4.DES中的5个工作模式、工作原理、优缺点

5.3DES优于2DES分析原因

6.对称加密、公钥体系加密密钥管理、安全性、可靠性。

7.RSA加密，过程、原理、安全性.

8.RSA加密的可行性分析。

9.Kerboros协议过程、安全行可行性分析。

**二、名词解释**

**第一章 概论**

1.计算机安全：对于一个自动化的信息系统，采取保护措施保证系统资源的完整性、可用性。

2.安全需求三元组——CIA

保密性C：对信息的访问和公开进行授权限制，包括保护个人隐私和秘密消息。

完整性I：防止信息被不恰当的修改或破坏，包括信息的不可否认性和真实性。  
可用性A：保证对信息的及时和可靠的访问和使用。

3.OSI安全框架

安全攻击 安全机制 安全服务

4.安全攻击：任何危及信息系统安全的行为

被动攻击：试图了解和利用系统信息但不破坏系统资源。（容易预防）

包括信息内容的泄漏和流量分析两种。

主动攻击：试图改变系统资源或影响系统的运作。（容易检测）

包括伪装、重播、消息修改、拒绝服务

5.安全机制：用来检测、阻止攻击，或从攻击状态恢复到安全状态的过程

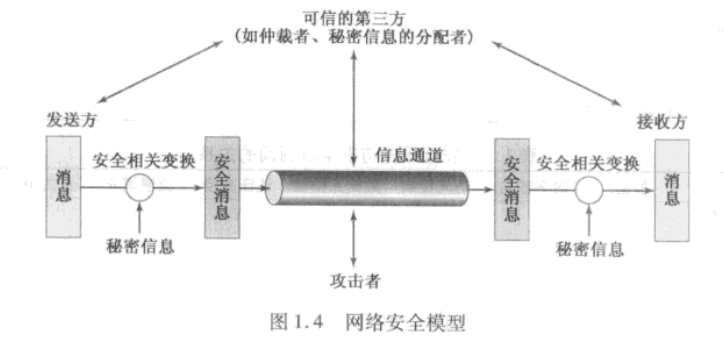
特定安全机制：加密、数字签名、访问控制、数据完整性、认证交换、流量填充、路由控制、公证；\*8

普通安全机制：可信功能、安全标签、事件检测、安全审计跟踪、安全恢复。\*5

6.安全服务：加强数据处理系统和信息传输的安全性的一种处理过程或通信服务。

五类：认证、访问控制、数据保密性、数据完整性、不可否认性

7.**网络安全模型**：



**第二章 传统加密技术**

1.**对称密码**：一种加解密使用相同密钥的密码体制。解密算法是加密算法的逆过程。使用代替和置换技术。其安全性依赖于所持有密钥的安全性。

五要素：明文、加密算法、密钥、密文、解密算法

2.攻击密码系统的两种通用方法：

①基于密码算法性质的密码分析

②基于穷举密钥的穷举攻击

3.**穷举攻击**：攻击者对一条密文尝试所有可能的密钥，直到把它转化为可读的有意义的明文。

4.无条件安全：一个密码体制无论有多少可以使用的密文，都不足以唯一的确定密文所对应的明文，则称该加密体制是无条件安全的。

5.**计算安全**：满足以下两个条件

①破译密码的代价超出密文信息的价值；

②破译密码的时间超出密文信息的有效生命周期。

6.代替技术：将明文字母替换成其他字母、数字或符号的方法。

7.置换技术：有限元素的集合S的置换是S中所有元素的有序排列，且每个元素只出现一次。

8.Caesar密码：是一种代替密码，就是将字母表中的每个字母，用它之后的第k个字母来代替。

加密： 解密：

3个特征：①加解密算法已知；②只有25个密钥；③明文所用的语言是已知的，且其意义易于识别。

9.单表代替密码：每条消息用一个字母表（给出明文字母到密文字母之间的映射）来加密。

10.Playfair密码：一种多字母代替密码体制。其密钥是基于一个密钥词构成的5\*5字母矩阵。一次加密两个字母，加密规则如下：

①两个相同连续字母需填充；②同行（右）/同列（左）；③一般字母对

11.多表代替密码：明文消息中采用不同的单表代替。

12.**一次一密**：使用与消息一样长且无重复的随机密钥来加密消息，密钥只对一个消息进行加密，之后丢弃不用。

13.置换加密：对明文进行置换的加密方法，密钥是其置换方式。（不同于置换技术）

**第三章 分组密码和数据加密标准**

1.**分组密码**：一种加/解密算法，其将输入的明文划分为固定长度的块（即分组），对每个分组做相同的加/解密处理，输出一个等长的密文分组，Feistel结构是其主要使用的结构。典型的分组大小为64位和128位。

分组密码算法实际上就是在密钥控制下，来实现对明文分组的加密变换。

为了保证密码算法的安全强度，分组密码算法必须满足以下要求：分组长度足够大、密钥量足够大、密码变换足够复杂。

2.**流密码**：一种加/解密算法，每次加密数据流的一个位或一个字节，通常使用密钥作为种子产生伪随机序列，然后将明文和该序列进行异或产生密文，密文与该序列异或即解密。适合远程终端输入等应用。

3**.Feistel加密结构特征**：加密算法的输入是最长为2w位的明文分组和密钥k。明文分组被分为等长的两部分：和。这两半数据经过n轮迭代后组合成密文分组。第i轮迭代的输入和来自上轮迭代的输出；而输入的子密钥是由整个密钥K推导出的。

每轮迭代都有相同的结构：代替作用在数据的左半部分，这种代替是通过轮函数F作用于数据右半部分后，与左半部分进行异或来完成的。代替之后，交换数据的左右两半完成置换。

4.Feistel结构的具体实现所使用的参数和特征：

参数：分组长度、密钥长度、迭代轮数、子密钥产生算法、轮函数F；\*5

特征：快速软件加/解密；简化分析难度

5.乘积密码：一次使用两个或两个以上的基本密码，所得结果的密码强度将强于所有单个密码的强度。

6.两种对付传统分析的方法：扩散和混淆

扩散：尽可能使明文和密文之间的统计关系变的复杂，以挫败推导出密钥的企图；

混淆：尽可能使密文和密钥之间的统计关系变的复杂，以阻止攻击者发现密钥。

7.**数据加密标准DES**：是使用最广泛的分组加密算法，速度较快，适用于加密大量数据的场合。

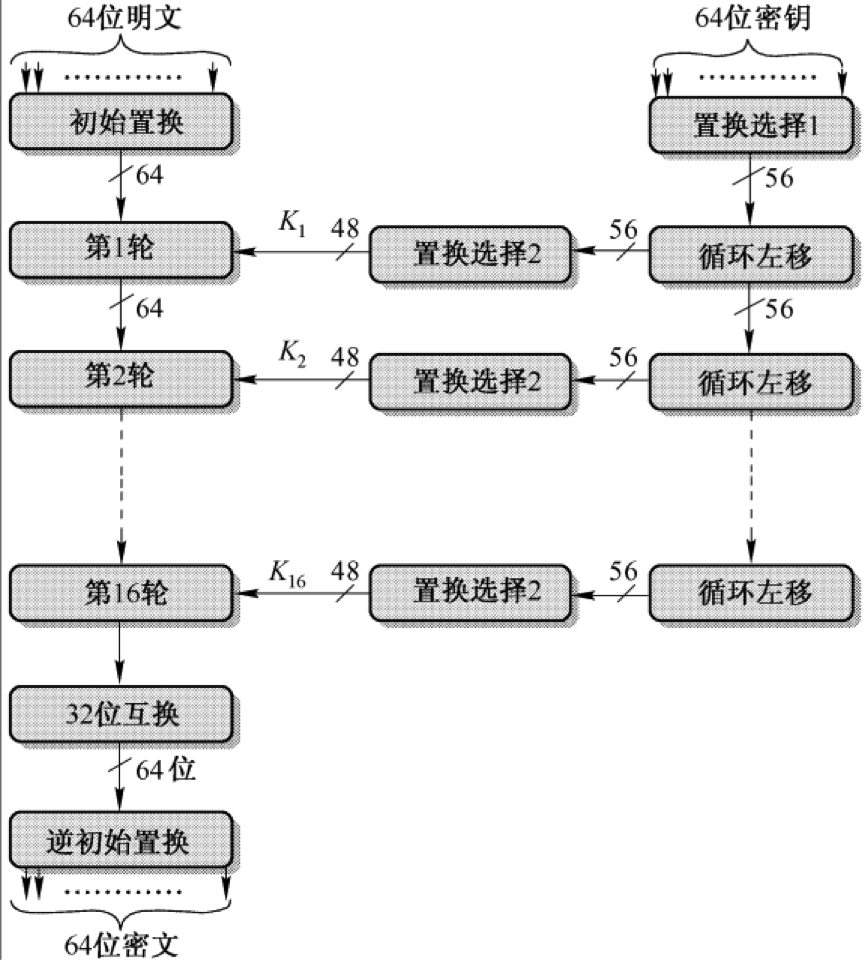
DES算法的入口参数有三个：密钥、明文分组、模式。

工作过程：

首先 64位明文分组经过初始置换（IP）而被重新排列；

然后 进行16轮相同函数的作用，每轮都有置换和代替，最后一轮迭代的输出有64位，它是输入明文和密钥的函数。其左半部分和右半部分互换产生预输出；

最后 预输出被逆初始置换后产生64位密文。



8.DES算法中S盒的作用：

S盒，即密钥置换盒，用在分组密码算法中，是非线性结构，其密码强度直接决定了密码算法的好坏。功能就是一种简单的代替操作。在DES中一个m\*n的S盒，需要n位输入，m位输出，用于模糊密钥和密文之间的关系。

S盒构造方法：随机选择、人为构造、数学方法构造

9.**雪崩效应：**明文或密钥的某一位发生变化会导致密文中的很多位发生变化。

10.差分分析和线性分析的区别

差 通过分析明文对的差值对密文对的差值的影响来恢复某些密钥比特。

线 对迭代密码的一种已知明文攻击，它利用的是密码算法中的“不平衡的线性逼近”。

**第四章 数论和有限域的基本概念**

1.模运算中的：

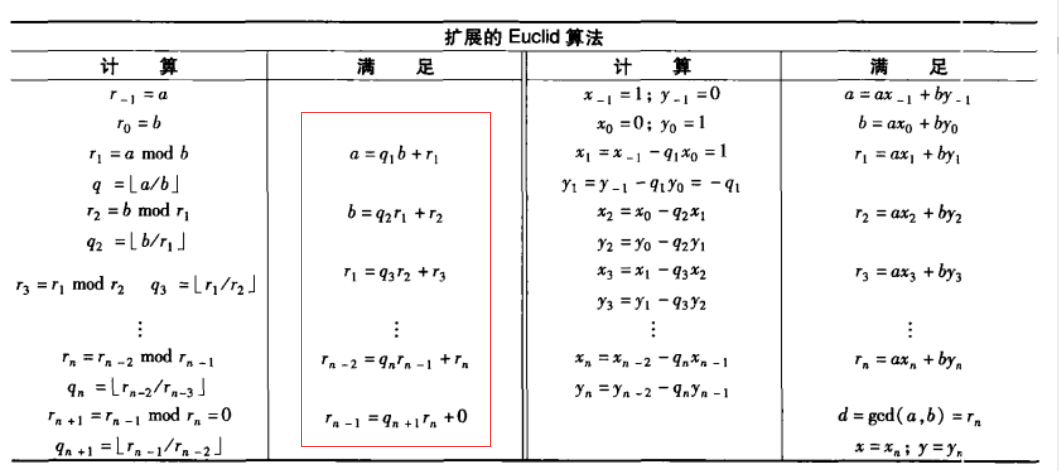
加法逆元：整数x的加法逆元y是使(x+y) mod n = 0成立的值；

乘法逆元：整数x的乘法逆元y是使(x\*y) mod n = 1 mod n成立的值。

2.**扩展的Euclid算法**

算法描述：给定整数a,b该法计算出gcd(a,b)以及x,y。满足：ax+by=d=gcd(a,b)，对于给定的整数a,b，ax+by的最小整数等于gcd(a,b)。

算法过程：

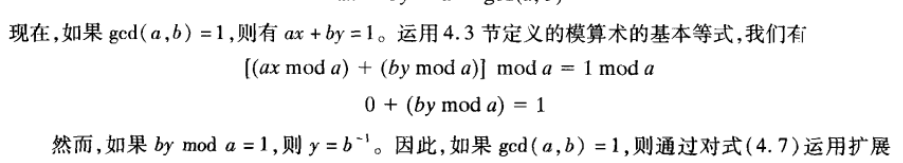


最好可以记住两个公式：



3.**在GF(p)中求乘法逆元：**

如果gcd(a,b)=1，那么b有模a的乘法逆元。使用扩展的Euclid算法来计算，得出的y即为所求。



**第五章 高级加密标准**

**1.高级加密标准AES：**

AES是一种分组加密算法。明文分组的长度为128位，密钥长度为128位、192位、265位。

输入：明文分组 密钥

加/解密算法的输入是一个128的明文分组，这个分组被组织成4\*4的字节方阵，这个分组被复制到state数组，在加/解密的各个阶段被修改。

密钥也被描述为字节的方阵，128位的密钥最终被扩展为44字的序列。

工作过程：

密码由N轮组成。在第一轮前有一初始变换（轮密钥加）；前N-1轮都由四种不同的变换组成：字节代替、行位移、列混淆、轮密钥加；最后一轮仅包含三个变换（没有列混淆）。每轮变换输入一个或多个4\*4的矩阵，并输出一个4\*4的矩阵，最后一轮输出的为密文。

2.AES的变换函数：

字节代替：用一个S盒完成分组中字节到字节的代替

行位移：一个简单的置换

列混淆：利用域GF()上的算数特性的一个代替

轮密钥加：当前分组和扩展密钥的一部分进行按位XOR

**第六章 分组密码的工作模式**

1. 多重加密：是将一个加密算法多次使用的技术。在第一次使用中，明文通过加密算法转换成密文，然后将该密文作为输入重新执行该加密算法，该过程可以重复任意多次。

2.2DES：是在两个阶段使用DES加密的一种形式最简单的多重加密算法。这种算法的密钥长度为56\*2=112位，密码强度增强了。

3.3DES：3DES是在三个阶段用DES算法的一种多重加密算法，共用到两组或者三组密钥。

4.中间相遇攻击：

假设： 则有：

给定明文对(P,C)，攻击如下：首先，将P按所有可能的密钥K1加密，得到个结果，按X的值排序放在一个表里。然后，将C按所有可能的密钥K2解密，每解密一次就将结果与表中的值比较，如果有相等的，就用刚才测试的两个密钥对一个新的明密文对进行验证。如果有两个密钥产生了正确的密文，就认定这两个密钥是正确的密钥。

5.IV：

初始向量，是和密文具有相同长度的数据分组。IV必须为收发双方共享，但第三方不能预测，可以先用ECB加密IV然后再发送。

**第七章 伪随机数的产生和流密码**

1.RC4：是一个可变密钥长度，面向字节操作的流密码，以随机置换作为基础。用密钥生成随机数与明文做异或，当密钥长度相当时，流密码可以与分组密码一样安全。

2.设计流密码要考虑的因素：

①加密序列的周期要长

②密钥流应尽可能接近真正随机数流的特征

③伪随机数发生器的输出受输入密钥的调节

**第八章 数论入门**

1.费马定理：若p是素数，a是正整数且不能被p整除，则。【互素】

另一种表示：若p是素数且a是任意正整数，则。【不要求互素】

2.欧拉函数：表示小于n且与n互素的正整数的个数。

定义 对素数p，有：=p-1



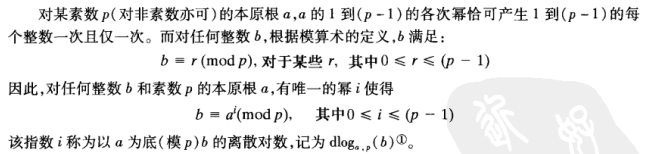
3.欧拉定理：对任意互素的a和n，有。【互素】

另一种表示：。【不要求互素】

4.中国剩余定理CRT：说明某一范围内的整数可通过它的一组剩余类数来重构，这组剩余类数是对该整数用一组两两互素的整数取模得到的。

5.本原根：如果一个数的阶为，则称之为n的本原根。

6.离散对数：



**第九章 公钥密码学和RSA**

1.非对称加密/公钥密码：这种密码体制使用两个密钥来进行加密和解密，这个两密钥分别是公钥和私钥。公钥和私钥是一对，如果使用公钥对数据进行加密，只有用对应的私钥才能解密，如果用私钥进行加密，只有用相应的公钥才能解密。因为加/解密使用两个不同的密钥，所以这种算法叫做非对称算法。

公钥密码体制的6个组成部分：

明文、加密算法、公钥、密钥、解密算法、密文 \*6

2.公钥密码体制的应用：

①加密/解密：发送方用接收方的公钥对消息进行加密。

②数字签名：发送方用其私钥对消息“签名”，签名可通过对整条消息加密或对消息的一个小的数据块加密来产生，其中该小数据块是整体整条消息的函数。

③密钥交换：通信双方交换会话密钥。

3.为得到安全算法，公钥密码体制应满足那些要求

①公/密钥的产生在计算上是容易的 （密钥生成）

②已知公钥和待加密信息，发送方产生相应密文在计算上是容易的（加密）

③接收方使用其私钥对接收的密文解密以恢复明文在计算是容易的（解密）

④已知公钥，攻击者要确定私钥在计算上是不可行的（公钥->私钥）

⑤已知公钥和密文，攻击者要恢复明文在计算上是不可行的

4.单向函数：每个函数值都存在唯一的逆，并且计算函数值是容易的，但求逆却是不可行的。

5.单向陷门函数：一个函数，若计算函数值很容易，并且在缺少一些附加信息时计算函数的逆不可行，但是已知这些附加信息时，可在多项式实践计算出函数的逆，称这样的函数为单向陷门函数。

6.RSA可能遭受的攻击

①穷举攻击

②数学攻击

③计时攻击

④选择密文攻击

**第十章 密钥管理和其他公钥密码体制**

1.Diffie-Hellman密钥交换(DH协议)：是一种安全协议，它可以让双方在没有对方任何预先信息的条件下通过一个不安全信道建立起一个密钥。这个密钥可以在后续的通讯中作为对称密钥来加密内容。这个密钥交换协议只能用于密钥的交换，而不能进行消息的加密和解密。

2.中间人攻击MITM：是一种“间接”的入侵攻击，这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就被称为“中间人”。

3.ElGamal密码体系：是一种较为常见的加密算法，它是基于1984年提出的公钥密码体制和椭圆曲线加密体系。既能用于数据加密也能用于数字签名，其安全性依赖于计算有限域上离散对数这一难题。在加密过程中，生成的密文长度是明文的两倍，且每次加密后都会在密文中生成一个随机数K，在密码中主要应用离散对数问题的几个性质：求解离散对数（可能）是困难的，而其逆运算指数运算可以应用平方-乘的方法有效地计算。也就是说，在适当的群G中，指数函数是单向函数。

4.椭圆曲线算法？？？看不懂……

**第十一章密码学Hash函数**

1.密码学Hash函数的作用：将可变长度的消息映射为固定长度的Hash值或消息摘要。要求一下两种情况在计算上不可行：

①（单向性）对预先指定的Hash值，找到对应的数据块

②（抗碰撞性）找到两个不同的数据块对应相同的Hash值

2.消息认证：是用来验证消息完整性的一种机制，能发现对消息的篡改和假冒。使用对称算法可以产生消息鉴别码MAC，使用公钥算法可以对消息进行签名。

3.数字签名：是一种认证机制，它使得消息的发送方可以添加一个起签名作用的码字。通过计算消息的Hash值并用发送方的密钥加密Hash值来获得签名。消息保证了消息的来源和完整性。

4.MD5：哈希算法的一种，常用于文件的唯一标识。用于确保信息传输完整一致。MD5的作用是让大容量信息在用数字签名软件签署私人密钥前被"压缩"成一种保密的格式（就是把一个任意长度的字节串变换成一定长的十六进制数字串）

5. SHA1:：是使用最广泛的hash算法的一种，建立在MD4只上，输出为160位hash值。

安全哈希算法主要适用于数字签名标准里面定义的数字签名算法。对于长度小于2^64位的消息，SHA1会产生一个160位的消息摘要。当接收到消息的时候，这个消息摘要可以用来验证数据的完整性。在传输的过程中，数据很可能会发生变化，那么这时候就会产生不同的消息摘要。

**第十二章 消息认证码**

1.消息认证码MAC：是一种需要使用密钥的算法，以可变长度的消息和 作为输入，产生一个认证码。拥有认证码的接收方能够计算认证码来验证消息的完整性。

2.构造MAC的方法：

第一种是将密码学hash函数以某种方式和密钥捆绑起来。

第二种是使用对称分组密码，将可变长度的输入转为固定长度的输出。

3.HMAC：利用现有的hash函数，加入密钥作为输入，用作mac的生成，就是HMAC。HMAC是密钥相关的哈希运算消息认证码，HMAC运算利用哈希算法，以一个密钥和一个消息为输入，生成一个消息摘要作为输出。把HASH值和一个Key结合起来既能用当前的HASH函数，又易升级为新的HASH函数，并能保持和散列函数一样安全性。简单，并易进行密码学分析。利用hash函数从报文和密钥产生MAC码，先计算特征，再把特征加密，或直接把散列函数和key结合得MAC。

4. 网络通信可能受到的攻击:

①泄密: 将消息透漏给没有合法秘密钥的任何人或程序。

②传输分析: 分析通信双方的通信模式

③伪装: 欺诈源向网络中插入一条消息

④内容修改: 对消息内容的修改，包括插入、删除、转换和修改。

⑤顺序修改: 对通信双方消息顺序的修改，包括插入、删除和重

⑥计时修改: 对消息的延时和重放。

⑦发送方否认: 发送方否认发送过某消息

⑧接收方否认: 接收方否认接收到某消息

5.基于密码的消息认证码CMAC

**第十三章 数字签名**

1.数字签名：是一种队证机制， 它使得消息的产生者可以添加一个起签名作用的码字。通过计算消息的散列值并用产生者的私钥加密散列hash值来生成签名，签名保证了信息的来源和完整性。

2.数字签名的特征：

①它必须能够验证签名者、签名日期和时间

②它必须能够认证被签的消息内容

③签名应能有第三方仲裁，以解决争议

3.时间戳

4. 动态口令牌：“中银e令”，即动态口令牌是一种内置电源、密码生成芯片和显示屏、根据专门的算法每隔一定时间自动更新动态口令的专用硬件。基于该动志密码技术的系统又称一次一密(OTP) 系统，即用户的身份验证密码是变化的，密码在使用过一次后就失效，下次登录时的密码是完全不同的新密码。作为一种重要的双因素认证工具，动态口令牌被广泛地运用于安全认证领域。动态口令牌可以大大提升网上银行的登录和交易安全。

**第十四章：密钥管理和分发**

1.端到端加密：存在于两个程序的进程之间，只是在源和目的两端架设保密设备，只能加密有效数据部分，适合公共商用网络。

2.会话密钥：是保证用户跟其它计算机或者两台计算机之间安全通信会话而随机产生的加密和解密密钥。会话密钥从密钥分发中心得到。会话密钥有时称对称密钥，因为同一密钥用于加密和解密。由于其大部分安全性依赖于其使用时间的短暂性，会话密钥常常频繁更改。各个消息可能使用不同的会话密钥。

3.公钥证书：指的是利用数字签名技术将用户的真实身份和用户的公开密钥进行有效绑定而形成的数字身份证明。X509标准是数字证书规范的标准。公钥证书保证公钥的安全性。

4.密钥分发：密钥分发的功能是给想要交换安全加密数据的双方分发密钥,并提供密钥安全分发所需要的方法或者协议。密钥分发常包括双方之间的频繁使用且长期存在的主密钥以及临时使用的会话密钥。

5.密钥管理：

6.X.509证书：X509定义了X500用户目录的一个认证服务框架。X.509是关于整数结构和认证协议的一种重要的标准，被广泛用于各种各样的应用中。X509是基于公钥密码体制和数字签名的服务。

7.签证机构CA：又称为证书授证（Certificate Authority）中心，作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。（证书管理机构）

每个用户自己产生一对公钥和私钥，并把公钥提交给CA申请证书。CA以某种可靠的方法核对申请人的身份及其公钥，并用自己的私钥签发证书。CA中心为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA机构的数字签名使得攻击者不能伪造和篡改证书。它负责产生、分配并管理所有参与网上交易的个体所需的数字证书，因此是安全电子交易的核心环节。

【注意数字证书和数字签名的差别】：

数字证书是由权威机构－－CA证书授权（Certificate Authority）中心发行的，能提供在Internet上进行身份验证的一种权威性电子文档，人们可以在互联网交往中用它来证明自己的身份和识别对方的身份。

数字签名是一种认证机制，它使得消息的发送方可以添加一个起签名作用的码字。通过计算消息的Hash值并用发送方的密钥加密Hash值来获得签名。消息保证了消息的来源和完整性。

数字证书好比身份证；数字签名好比签字。

8. 公钥基础设施(PKI)被定义为由软件、人、策略和程序构成的一整套体系。这些程序用来创建、管理、有储分发和撒销 建立在非对称密码算法之上的数字证书。

**第15章 用户认证**

1.双向认证/相互认证：相互认证协议可以使通信双方确信对方的身份并交换会话密钥。

2.重放攻击：又称重播攻击、回放攻击，是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的。主要用于身份认证过程，破坏认证的正确性。重放攻击可以由发起者，也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据，之后再把它重新发给认证服务器。

3.Kerberos：在一个分布式环境中，用于服务器与用户之间的相互认证的协议。

解决方案：在一个分布式的Client/Server体系机构中，引入一个可信任的第三方（Kerberos服务器），让其提供认证服务；采用共享密钥加密技术。（与其他认证不同的是Kerberos仅仅依赖于对称加密体制而未使用公钥加密体制）

**三、简答题**

**1.凯撒密码和现代密码的区别，如何改进成现代密码？**

有区别：

①凯撒密码的密钥空间中只有26个密钥

②作为一种分块加密算法（一个字符一个字符加密，本质上是分块），他本质上使用了一个有序的P盒，没有使用S盒。

③不安全，如果已知加密算法，凯撒密码用穷举攻击是很容易攻破的，只需简单测试25中可能的密钥，而现代密码，推导密钥的难度比凯撒密码大，安全性更好。

【如何改进成现代密码】

可以参考书中的

**2.分组加密算法与流加密算法的比较**

①分组加密每次加密一个明文分组即8字节；流加密每次加密一位或一个字节；

②分组加密对相同的明文分组总是产生相同的密文分组；而流加密却输出不同的密文比特；

③流加密一般很快

3. **3DES vs 2DES，原因**

3DES更安全

2DES是在两个阶段使用DES加密，使用两个密钥，加密过程：，这种方法的密钥长度为56\*2，密码强度增加了，但是存在两个问题：一是约化为单次加密的风险，那么不管加密多少次都等同于用一个密钥进行一次DES加密的效果；二是中间相遇攻击的风险。

3DES的运算过程是加密-解密-加密，很好的解决了2DES存在的问题，而且使用三个密钥的3DES的密码强度更强，所以3DES要优于2DES

**4. DES中的5个工作模式、工作原理、优缺点**

**ECB**：DES和AES五种工作模式之一，电码本模式。直接利用加密算法对数据加密。它一次独立处理一个明文分组，每次使用相同的密钥加密。

优点：并行加密，随机存取。

缺点：相同明文分组对应相同密文分组，暴露统计规律。

应用：单个数据的安全传输（比如一个加密密钥）。

**CBC**：DES和AES五种工作模式之一，密文分组链接模式。这种模式下加密算法的输入是当前的明文组和上一个密文组的异或，而使用的密钥是相同的。并且，CBC模式如果最后的分组不是完整的分组，则需要填充至b位的满分组。解密时，每个密文分组分别进行解密，再与上一块密文异或就可以恢复成明文。

优点：避免明密对应，可用作认证。

缺点：不能并行加密随机存取。需要初始化IV向量。等待缓冲区满8bit，否则需要做填充。

应用：适合加密长度大于b位的消息

**CFB**：DES和AES五种工作模式之一，密文反馈模式。一次处理s位，上一块密文作为加密算法的输入，产生的伪随机数输出与明文异或作为下一单元的密文。

优点：可以使用不同的初始化变量使相同的明文产生不同的密文，防止字典攻击；无填充

缺点：一旦某位数据出错,会影响目前和其后8个块的数据

应用：面向数据流的通用传输；认证

**OFB**：DES和AES五种工作模式之一，输出反馈模式。一次处理一个分组，加密算法的输入是上一次加密的输出，

优点：传输过程中在某位上发生的错误不会影响其他位；无填充

缺点：抗消息流篡改攻击的能力较弱

应用：噪声信道上的数据流的传输

**CTR：**DES和AES五种工作模式之一，计数器模式。每一个明文分组都与一个经过加密的计数器异或。对每个后续的分组，计数器递增。

优点：硬件效率；软件效率；预处理；随机访问；可证明安全性；简单性；无填充

缺点：

应用：面向分组的通用传输；用于高速需求

**5.为什么流密码使用相同密钥不好？**

如果流密码对两个明文进行加密且使用相同的密钥，则密码的分析会相当容易。如果对两个密文进行异或，那么得出的结果就是两个原始明文的异或。如果明文是已知特征的字节流，则密码分析极易成功。

**6.Miller-Rabin测试可确定一个数不是素数，但不能确定一个数是素数。该算法如何用来进行素性测试？**

重复使用Miller-Rabin算法。对随机选择的a，重复调用TEST(n)，如果某时刻TEST返回“合数”，则n一定不是素数；若TEST连续t次返回“不确定”，这样当t足够大时，我们可以相信n是素数

7. RSA加密，过程、原理、安全性

过程：对明文分组M和密文分组C，加/解密的过程如下



其中发送双方均已知n，发送方已知e，只有接收方知道d，故公钥为PU={e,n}，私钥为PR={d,n}.

原理：RSA算法是一种分组密码，其明文和密文都是0-n-1之间的整数，通常n的大小为1024位二进制数或者309位十进制数。

【原理补充】

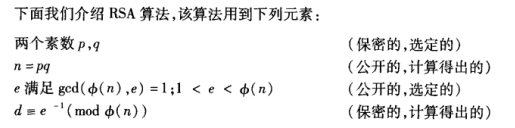
安全性：对RSA算法的攻击可能有4中方式：穷举攻击、数学攻击、计时攻击、选择密文攻击

RSA的安全性依赖于大数的因子分解，这样攻击RSA系统的难度就是大整数因子分解的难度，一般认为这是一个NPC问题，尽管尚未在理论上证明分解因子的问题一定困难，但千百年来经过众多学者的研究，迄今没有找到一种有效算法，绝大多数数论学家倾向于认为不存在大整数因子分解的多项式算法，因此目前这一破译只能依赖于现代的计算机技术，用程序进行尝试分解，从而对大数的因子分解.不过随着计算机运算速度的提高和并行计算的发展，加上因子分解方法的改进，低位数的密钥的破解已成为可能.因子分解需的时间随密钥长度的增加而成指数指增加，只要n的长度达到一定要求，并且参数p,q和e选取恰当的话，RSA系统是相当安全的.

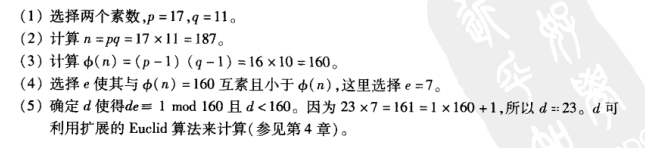
8. RSA加密的可行性分析。

我一直不会……考试的时候考了。写的是RSA密码的安全性基于大整数的素分解，还有使用欧拉函数和欧拉定理提供正确性……

9.RSA原理 给p,q,e,c，求d和m。



【例】



然后进行解密：计算M

【例】

**10.公钥体系、对称加密体系、MAC、HASH、数字签名在认证上的作用、特点**。

认证可以分为身份认证和消息来源认证。身份认证一般使用使用CA(证书授权中心)，CA用到了数字签名，而数字签名一般使用公钥算法；消息认证则使用MAC，MAC在工业实现中一般先把消息hash到固定长度再计算认证码，而hash函数的实现中可能使用到了对称加密算法。另外Kerberos协议使用对称加密算法实现了消息来源认证。

**11.对称密码和公钥密码的区别**

①密钥上，对称密码加解密使用相同的密钥，而公钥密码则使用发送方产生的两个密钥分别加解密；

②算法上，对称密码主要是使用代替和置换这两种加密技术；而公钥算法则是使用数学方法来进行加密。

③安全性要求：

对称密码：密钥必须保密；没有密钥，解密不可行；知道算法和若干密文不足以确定密钥

公钥密码：两个密钥之一必须保密；无解密密钥，解密不可行；知道算法和其中一个密钥以及若干密文不能确定另一个密钥

**12 .防止重放攻击方法。**

①序列号：对于每一个用于认证交互的消息附上一个序列号，新的消息只有其序列号满足适当的顺序时才会被接收，但是这种方法要求每一方都跟踪记录与其交互的通信双方的最新序列号，开销很大。

②时间戳：只有当消息包含一个时间戳时，接收方才接收消息。该时间戳有接收方进行判断，要接近于接收方所知的当前时间。该方法要求不同参与者之间的时钟是同步的，且不适合于面向连接。

③挑战/应答：A想要一个来自B的新消息，首先发给B一个临时交互号（询问），并要求后面从B接收的消息（回复）包含正确的临时交互号。这种方法不适合于无连接。

**13.Kerberos协议过程、安全行可行性分析。**※

这个肯定是要考的，看版本4 同一个域中的就行了。