问答

1.请简述数字签名的含义及其基本特征。

数字签名（digital signature) 是一种给电子形式存储的消息签名的方法。正因为如此，签名之后的消息能够通过计算机网络传输。数字签名是手写签名的数字化形式，与所签信息"绑定"在一起。具体地讲，数字签名就是一串二进制数。 它应具有下列基本特性：

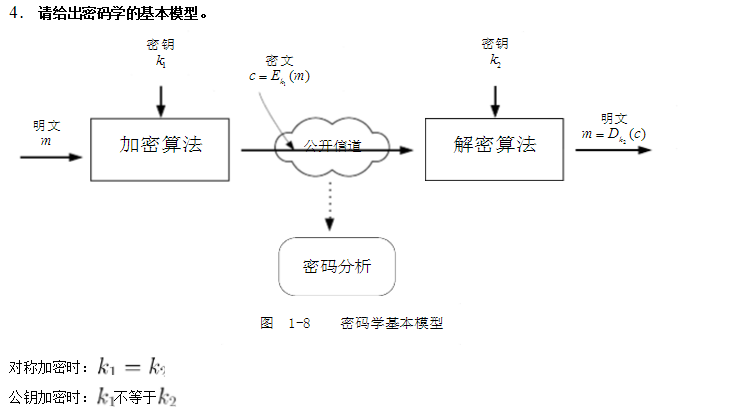
1) 签名可信性：其他人可利用相关的公开消息验证签名的有效性；

2) 不可抵赖性：签名者事后不能否认自己的签名；

3) 不可复制性：即不可对某一数字内容或消息(message)的签名进行复制；数字签名文件本身可以复制，因此，签名文件本身应该包含诸如日期、时间在内的信息以防止签名被复制.

4) 不可伪造性：任何其他人不能伪造签名者的签名。或者说，任何其他人不能找到一个多项式时间的算法来产生签名者的签名；

2.



3. 利用本学期所学知识，设计一文件安全传输方案

参考答案：以终端A为发送方，终端B为接收方为例，实现流程大致应如下。 终端A操作：

1) 与终端B预先协商好通信过程中所使用到的对称加密算法、非对称加密算法和哈希函数；

2) 采用对称加密算法（密钥称之为会话密钥）对传输信息进行加密得到密文，确保传输信息的保密性；

 3) 使用终端B的公钥对会话密钥进行加密，确保传输信息的保密性以及信息接收方的不可否认性；

4) 采用哈希函数（生成文件摘要）确保传输信息的完整性，并使用自己的私钥对文件摘要进行签名（得到数字签名），确保信息发送方的不可否认性；

5) 将密文、加密后的会话密钥和数字签名打包封装（放到一起）后，通过网络传输给终端B。

 终端B操作：

1) 与终端A预先已协商好通信过程中所使用到的对称加密算法、非对称加密算法和哈希函数；

2) 使用自己的私钥对终端A加密的会话密钥进行解密，得到准会话密钥；

3) 使用准会话密钥对得到的密文进行解密，得到准明文；

4) 使用终端A的公钥对得到的数字签名进行解密，得到准明文摘要；

5) 使用哈希函数计算得到准明文摘要；

6) 将计算得到的摘要与准明文摘要进行比较，若相同则表明文件安全传输成功。

1、安全基本目标有哪些？其含义分别是什么？（P7）   
1)保密性：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信息。保密性缺失的定义是信息的非授权泄露；   
2)完整性：防止对信息的不恰当修改或破坏，包括确保信息的不可否认性和真实性。完整性缺失的定义是对信息的非授权修改和毁坏；   
3)可用性：确保对信息的及时和可靠的访问与使用。可用性的缺失是对信息和信息系统访问与使用的中断。

尽管CIA三元组足以定义安全目标，但是许多从事安全领域研究的人认为还需要其他概念来定义才更全面。下面是其中两个被提及较多的概念：   
真实性：一个实体是真实性的、是可被验证的和可被信任的特性；对传输信息来说，信息和信息的来源是正确的。也就是说，能够验证那个用户是否是他声称的那个人，以及系统的每个输入是否均来自可信任的信源。   
可追溯性：这一安全目标要求实体的行为可以唯一追溯到该实体。这一属性支持不可否认性、阻止、故障隔离、入侵检测和预防、事后恢复、以及法律诉讼。

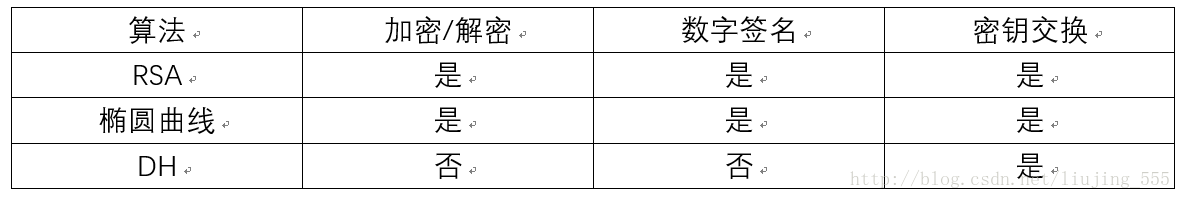
2、 OSI安全框架定义了哪三个方面？（P9）其中安全攻击被分成哪两个类别，有什么特点？分别有哪些实例？(P10)

（1）OSI安全框架可以简短地定义如下：   
①安全攻击：任何危及信息系统安全的行为；   
②安全机制：用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程（或实现该过程的设备）   
③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。其目的在于利用一种或多种安全机制进行反攻击

（2）安全攻击被分为被动攻击和主动攻击两种   
被动攻击的特点：对传输进行窃听和监测，攻击者的目标是获得传输的信息，难以检测，但可以防止。   
实例：信息内容的泄露、流量分析。   
主动攻击：包括对数据流进行修改或伪造数据流，难以绝对预防，但容易监测   
实例：伪装、重播、消息修改、拒绝服务

3、 现代密码算法主要包括哪两种？其中对称密码算法按照对明文的处理方式不同可以分成哪两类?常见的对称密码算法有哪些？基本的参数 (明密文分组长度，密钥长度) ？公钥密码有哪些算法，主要的应用是什么？（见书197）   
（1）现代密码算法：对称密码算法、公钥密码算法   
（2）分组密码和流密码   
（3）DES和AES   
（4）

  
（5）

  
（6）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”。签名可以通过对整条消息加密或者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条消息的函数   
③密钥交换：通信双方交换会话密钥。有几种不同的方法可以用于密钥交换，这些方法都使用了通信一方或双方的私钥

4、分组密码的工作方式有哪些?（P135-143）   
（1）电码本模式   
（2）密文分组链接模式   
（3）密文反馈模式   
（4）输出反馈模式   
（5）计数器模式   
（6）用于面向分组的存储设备的XTS-AES模式

5、 公钥算法安全性的数学基础有哪些？（P61）   
素数、费马定理、欧拉定理、素性测试、中国剩余定理、离散对数

6、什么是消息认证？如何实现消息认证（或消息认证函数的实现方式）？(P272)   
（1）消息认证就是验证所收到的消息确实是来自真正的发送方，且是未被修改的消息。它也饿验证消息的顺序和及时性。

（2）①Hash函数：将任意长的消息映射为定长的Hash值的函数以该Hash值作为认证符   
②消息加密：对整个消息加密后的密文作为认证符

7、 散列函数（就是哈希函数）可被应用于哪些方面？(P239)密码学散列函数需哪些安全性需求？(P245)常见的散列函数有哪些？(P251)基本参数（输入、输出长度、安全性等）？什么是生日攻击？   
（1）消息认证、数字签名、其他应用（产生单向口令文件、入侵检测和病毒检测、构建随机函数（PRF）或用作伪随机数发生器（PRNG））。   
（2）①输入长度可变：函数H可应用与任意大小的数据块   
②输出长度固定：H产生定长的输出   
③效率：对任意给定的x，计算H（x）比较容易，用硬件和软件均可实现   
④抗原像攻击（单向性）：对任意给定的Hash码h，找到满足H（y）的y在计算上是不可行的   
⑤抗第二原像攻击（抗弱碰撞性）：对任何给定的分块x，找到满足y!=x且H(x) = H(y)的y在计算上是不可行的   
⑥ 抗碰撞攻击（抗强碰撞性）：找到任何满足H(x) = H(y)的偶对(x,y)在计算上是不可行的   
⑦伪随机性：H的输出满足伪随机性测试标准   
前三个是Hash函数实际应用的需求   
满足前五个称为弱哈希函数

（4） 常见的散列函数：SHA-512、SHA-3

（5）   
（6） 生日攻击：   
利用“两个集合相交”问题的原理生成散列函数碰撞，达到目的的攻击称为生日攻击，也称为平方根攻击。   
它依赖于Hash值的长度。只要Hash码较短（如不超过64位）或Hash码很长但可以分解为独立的子码，就存在有生日攻击。

8、消息认证码（密码校验或MAC）的实现方式有哪两种？常见的算法有哪些？   
（1）基于Hash函数的MAC、基于分组密码的MAC   
（2）基于Hash函数的MAC：HMAC算法   
基于分组密码的MAC：DAA（数据认证算法）和CMAC（基于密码的消息认证码）   
9、什么是数字签名？数字签名的作用是什么？常见的数字签名算法有哪些？如何理解RSA私钥加密实现数字签名?   
（1）数字签名是一种以电子形式存在于数据信息之中的，或作为其附件或逻辑上有联系的数据，可用于辨别数据签署人的身份，并表名签署人对数据信息中包含的信息的认可技术   
（2）数字签名有以下特征：   
①它必须能验证签名者，签名日期和时间；   
②它必须能认证被签的消息内容；   
③签名应能由第三方仲裁，以解决争执   
因此，数字签名具有认证功能   
（3）DSA算法   
ECDSA算法（椭圆曲线数字签名算法）   
RSA-PSS数字签名算法   
（4）发送方使用私钥加密后，接收方用公钥解密得到信息，能用发送方的公钥解密必定是用的发送方的私钥加密，便可以进行身份确认实现数字签名。

10、 对称密钥的分发方式有哪些（如何实现）？   
（1）A选择一个密钥后以物理的方式传递给B   
（2）第三方选择密钥后物理地传递给A和B   
（3）如果A和B先前或最近使用过一个密钥，则一方可以将新密钥用旧密钥加密后发送给另一方   
（4）如果A和B到第三方C有加密连接，C可以在加密连接上传送密钥给A和B   
实现方法：   
（1）A向KDC（密钥分发中心）发送包请求一个会话密钥来保护到B的逻辑连接安全，其中包括A、B的身份和该次传输的唯一标识N1，称为临时交互号   
（2）KDC返回的信息是用Ka加密的，因此只有A能读取该信息，并且A知道该信息是由KDC发来的。该信息中包括一次性回话密钥Ks和临时交互号。A可以知道该信息是否被更改过。还包括一次性会话密钥Ks和A的标识Ida。后面这两个消息由密钥Kb加密，发送给B以达到建立连接和检验A的身份。   
（3）A保存会话的密钥Ks，将E(Kb,[Ks||Ida])发送给B。   
（4）B使用全新的会话密钥Ks加密临时交互号N2并将结果发送给A   
（5）同样，A使用Ks加密f(N2)后发送给B，其中f是一个执行N2转换的函数   
注：实际的密钥分发方案只包括（1）到（3），（3）到（5）是执行认证功能   
11、 什么是公钥证书？如何生成？CA的作用包括哪些？PKI包括哪些关键元素？   
（1）公钥证书，通常简称为证书，是一种数字签名的声明，它将公钥的值绑定到持有对应私钥的个人、设备或服务的身份。通信双方使用证书来交换密钥，证书包含公钥和公钥拥有者的标识，整个数据块由可信任的第三方签名。   
（2）一个用户把它的公钥交给管理员，从而获得一个证书，接着用户就可以公开证书，任何需要知道该用户公钥的人都可以获得证书。   
（3）CA（签证机构）：是证书和证书撤销列表的发行人   
CA可以创建、发放证书，只有CA可以修改证书，证书使用CA私钥进行加密以签名，某些时候CA还会撤销证书。   
（4） PKI是Public Key Infrastructure的首字母缩写，翻译过来就是公钥基础设施；PKI是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范

在RSA体制中，某给定用户的公钥e=31，n=3599，那么该用户的私钥等于多少？（10分） 3031