**OSI安全框架：**

**安全性攻击：任何危及企业信息系统安全的活动**

**安全机制：用来检测、组织攻击或者从攻击状态回复到正常状态的过程，或实现该过程的设备**

**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。**

**安全攻击：**

被动攻击：试图了解系统的信息但不影响系统资源（消息内容泄露；流量分析）

主动攻击：试图改变……（伪装，重放，消息修改，拒绝服务）

安全服务:5类

认证；访问控制，消息保密性，消息完整性，抗抵赖性

**网络安全模型**：发送方（消息）-安全变换（加上秘密消息（可能是密钥）-安全消息-信息通道（可能有攻击者）-安全消息-安全变换（加上秘密消息（可能是密钥））-接受方（消息）

**网络访问安全模型**：黑客（希望保护信息系统不受有害的访问）

**2：传统加密技术**

攻击密码体制的典型目标是回复使用的密钥：两种方法：

**密码分析学；穷举攻击**

对加密消息的攻击类型：（算法必须是公开的）

**惟密文攻击**；已知明文攻击；选择明文攻击；选择密文攻击；选择文本攻击；

计算安全：破解的代价超出密文信息的价值；破译密码的时间超出密文的有效生命期

**一次一密**，密钥只对一个消息进行加解密，之后丢弃不用，每一条新的消息都需要一个与其等长的密钥，对于一个密文，给出任何一个与其等长的明文都可以找到一个密钥。

一次一密提供完全的安全性存在两个基本难点：

产生大规模随机密钥有实际困难；密钥的分配和保护

**3+4分组密码和数据加密标准 高级加密标准**

**Feistel Ciper:**

是一种用来设计对称密码算法的常用结构，通常采用多轮结果，每轮由密钥生成的本轮密钥参与，首先将分组明文分为左右两个部分，其中右半部分是经过一个由轮密钥参与的复杂含糊结果和左半部分异或作为本轮的输出，并作为下一轮的左半部分，左半部分将作为下一轮的右半部分。

Feistel结构具体实现依赖于：

分组长度

密钥长度；

迭代轮数；

子密钥产生算法；

轮函数；

使用feistel密码还有两个其他方面的考虑：

快速软件加解密和简化分析难度

Feistel体现出：

混淆：尽可能使明文和密文间的统计关系变得复杂，推导密钥比较难

扩散：使明文的统计特征消散在密文中

**DES**

**组密码，**数据加密标准 64位分组56位密钥 17轮置换

DES显示出很强的雪崩效应

雪崩效应：明文或密钥微小的改变将对密文产生很大的影响

**3DES**

三重数据加密算法，每个数据块用3次DES 增加了DES密钥长度，C=Ek3(Dk2(Ek1(P))) P=Dk1(EK2(Dk3(C)))，可以用两个或三个密钥

**AES**

高级加密标准：AES

产生背景：des和3des其实够用；但是较慢，而且分组长度均为64

，可能有安全隐患，

高级加密标准，128位元 128/192/256位元加密，在4\*4字节矩阵上加密字节代替、行移位、列混淆、轮密钥加

**DES特点**：分组比较短、密钥太短，密码生命周期短、运算速度较慢。

安全特性：DES算法具有极高的安全性，到目前为止，除了用穷举搜索法对DES算法进行攻击外，还没有发现更有效的办法。

AES特点：安全；代码紧凑，速度够快，适合软硬件实现；结构简单；密钥大小可变

AES:分组长度为128位，支持128，192，256位的密钥

AES的数据结构由四个不同阶段组成：

字节代换：用一个s盒完成分组中的按字节代换；行移位：一个简单置换；列混淆；轮密钥加；

3DES特点： 实现方便，节省投资，DES模块本身不需要改变，只改变上层应用程序。

安全特性：是高强度的加密算法

适用场合：PGP、S/MIME、Mozilla

AES和DES的不同？（进而延伸为AES较DES在哪些方面有提高）？

1. 密钥的个数和长度不同（DES密钥是56位比较短，AES可以支持128，192和256位不同密钥的选择，安全性增强）
2. S盒构造不同，（DES的s盒是给出的，但是AES的S盒是利用算法来计算出来的）
3. DES的分组长度仅为64位，AES是128位（就效率和安全性来说，AES要好点）
4. AES是全处理的对于数据，Des是非对称处理，
5. AES加解密算法不一样，DES加解密算法是一样的
6. AES比DES更能抵抗穷举攻击
7. **AES显著特征是他不是feistel结构，在每一轮里面都使用代换和混淆**并行的处理整个数据分组

**6：对称密码的其他内容**

双重DES和多重DES

(9)什么是3DES,为什么不使用2DES，

通过三次使用DES算法串联，分别使用2个或三个密钥参与，比DES密钥长，更安全可靠，2DES存在中间相遇攻击，不安全(中间相遇攻击使用两组已知明密文对就可以猜出正确密钥的概率很大了，，已知明文攻击可以成功对付密钥长度为112位的双重DES,其付出是2^56数量级，比攻击单个DES所需的2^55数量级多不了多少

进行简单的一个解释：（从前往后加密，从后往前解密，两个数据集合进行比较，第一次相等，会产生2^112/2^64 = 2^48种错误结果，第二次再次相等降为2^48/2^64 = 2^-16,中间相遇攻击使用两组已知明密文对就可以猜出正确密钥的概率为1-2^-16很高）

**中间相遇攻击**

中间相遇攻击是生日攻击的一种变形，它不比较Hash值，而是比较链中的中间变量。这种攻击主要适用于攻击具有分组链结构的Hash方案。

构建在生日攻击基础上的，非64-1,而是64/2（说明）

使用64位的散列码，攻击者找到这样的消息大约需要2^32次尝试

说明：发送方用其私钥对m位的散列码加密并将加密后的三列码附于消息之后，攻击者产生该消息的2^m/2种便是，且每一种便是表达相同的意义，攻击者在伪造一条消息，并产生该伪造消息的2^m/2种变式，攻击者准备用伪造消息替代真实消息，比较上面两个集合，找出产生相同散码的一对消息，根据生日悖论，找到这对消息的概率大于0.5，如果找不到这样的消息，那么再产生一条有效消息和伪造的消息直至成功为止。

分组密码的工作模式及简单介绍：

分组密码的工作模式：（每一个工作模式具有的一些缺点和解决增强的办法）ECB：用相同的密钥分别对明文组加密，一次处理一组，每次使用相同的密钥，适用于单个数据的安全传输和加密密钥（非结构化）

应用:单个数据

缺点：比较容易利用结构特性破译（如果明文分组后有重复的话）；

CBC（密文分组链接）：加密算法的输入是上一个密文组和下一个明文组的异或。适用于普通目的的面向分组的传输，认证（CBC-MAC）之类；

缺点:加密太慢了

CFB:密文反馈：一次处理j位，上一块密文作为加密算法的输入，用产生一个伪随机数输出与明文异或作为下一块的输入，和CBC一样

缺点：在传输过程中某位发生错误，会继而影响其他的位发生错误。

OFB:输出反馈：与CFB基本上一样，只是加密算法的输入是上一次DES的输出：噪声频道上的数据流的传输（如卫星通信）；

优点：在传输过程中某位发生错误，不影响其他的位发生错误。

缺点：抗消息流篡改的能力不如CFB,密文中的某位取反，相应的，恢复出的明文某一位也取反。

CTR（计数器）：对每一个明文分组都与一个加密计数器相异或，对每个后续分组计数器递增：普通的面向分组的传输；用于高速需求

优点：硬件效率并行处理多块明文密文的加解密

为什么要选择工作模式：

选择工作模式是一项增强密码算法或者使算法适应具体应用的技术。

**RC4**

加密算法是密钥长度可变的流加密算法簇。之所以称其为簇，是由于其核心部分的S-box长度可为任意，但一般为256字节。该算法的速度可以达到[DES](http://baike.baidu.com/view/7510.htm)加密的10倍左右，且具有很高级别的非线性。

RC4特点：密钥长度可变

RC4:序列密码算法 速度快，但需要安全传递密钥 安全性比较高 应用于SSL和WEP协议

适用于：需要对数据流加密解密的应用：通过一个数据通信信道或者网页浏览连接

RC4未被广泛应用的原因：

密钥生成+存储困难，不安全（密钥需要无限长，无周期）

设计流密码需要考虑的主要因素：

加密序列的周期要长；密钥流应该尽可能接近于一个真正的随机数流的特征；随机数的输出依赖于输入密钥的值，为了防止穷举攻击，密钥的长度要尽可能长

**单向函数**：

每个函数值都存在唯一的逆，并且计算函数值是很容易的，但求逆是不可行的（容易是指可以在输入长度为多项式时间内得到解决）

**单向陷门函数：**

**一个函数，若极端函数值很容易，并且在缺少一些附加信息是计算函数的逆是不可行的，但是已知这些附加信息时，可在多项式时间内计算出函数的逆，称这样的函数为单向陷门函数。**

**7用对称密码实现保密性**

**端到端加密vs.链路层加密（概念，优点，缺点比较）**

**分布式环境中的加密设备可以支持链路加密和端对端加密，链路加密的没饿节点都需要一套加密设备，端对端加密只需在系统的两个中断执行加密和解密操作**

链路层加密：在通信链路两端都加上加密设备，链路上的信息传输可以是安全的。

缺点：每次分组交换都需要将消息解密（例如帧中继，因为交换时需要用到数据包头地址，以便寻路，消息易受攻击，共享一条链路的每对节点之间都要共享唯一密钥，整个网络中密钥数目很大

端对端加密：在两端西永中进行，由源主机和终端加密数据，密文经由网络传送到目的主机或终端。目的主机和源主机共享一个密钥以便解密（不可以加密包头）

缺点：如果不使用这种方法，无法对信息原实现认证

为了提高安全性，应该同时使用链路加密和端对端加密

在一段同质导线的两端,链路两端分别设置加密设备(硬件),要求所有线路段上都加密才行,可以加密整个包

密钥分配的几种方法：

1密钥由A选择，并亲自交给B

2第三方选择密钥，亲自交给AB

3如果以前两者或最近使用过某蜜月，其中一刚可以用它加密一个新密钥后再发送给另一方谨防密钥已经被窃取或丢失）

4A和B与第三方C均有秘密通道，则C可以将秘密发送给A和B

5KDC

**随机数的特性与用途；**

特性:均匀分布性，独立性，不可预测性

用途：作为密钥；DSA算法中选取；流密码需要有真的随机数；密钥分配时需要使用临时交互号来作为握手信息之一，为了防止重复攻击，使用随机数可以防止攻击者判断或者猜测临时交互号；会话密钥的产生；RSA公钥加密算法中密钥的产生

**9公钥密码学与RSA**

RSA算法的正确性+安全性证明；以及会计算明文，密文，以及在计算中的一些技巧问题（P191,P204）

RSA算法的可行性：

RSA算法首先是要找大素数：随机生出一个大数，可以利用miller\_rabin算法来判断其是否是素数，如果不是，在该数周围存在素数的概率很大，所以寻找到一个大素数是很容易的。

密钥协商differ-hellman算法：简述算法+正确性+缺点（只能用来产生密钥，不可以认证，可能会有伪造的安全性问题）（P213）

数字签名的一些属性:

DSA和RSA都可以构造数字签名，其不同之处在于：

RSA是确定性签名，只要给定消息，每一洗给出的签名值都是一样的，DSA是不确定的签名，因为引入了随机数，每一次产生的签名都是不一样的，因为每一次随机数不一样，这样可以避免重放攻击，RSA可以通过增加时间因素来弥补。

**数字证书**

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钥进行有效绑定而形成的数字身份证明，X509标准时数字证书规范的标准。

RSA:私钥的保密性，数字证书的构造机制如何实现公钥的真实性？

（CA）P210——P211

**10密钥管理和其他公钥密码体制**

公钥分配：

1公开发布 2公开可访问目录 3公钥授权 4公钥证书

公钥证书构造机制以及如何实现公钥的真实性

公钥证书的方法应该满足下列要求：

1任何通信方可以读取证书并确定证书拥有者的姓名和公钥

2任何通信方可以验证该证书出自证书管理员，而不是伪造的

3只有证书管理员可以产生并更新证书

4任何通信方可以验证证书的当前性

CA = E(PRauth,[T||IDA||PUa])

每一个通信方可以利用CA的公钥来解密，解开说明该该信息来自CA，可以信任，

Differ\_Hellman密钥交换

**11消息认证和散列函数**

认证函数：

可分为三类：

消息加密；MAC（消息认证码）：散列函数sansanl

**HMAC**

基于散列函数的MAC码算法，就是用Hash函数来设计MAC。

优势：其软件执行速度比DES这类的对称分组密码要快；有许多的共享密码学Hash函数代码库。

**CMAC:CBC-MAC密文分组链接消息认证码**

Hash函数的特性的用途

Hash函数是一种单向函数，它将任意长度的明文转换成定长的数据，用于认证，签名，产生伪随机数，保证数据的完整性，hash函数常用来唯一标识一个文件，它满足单向性，强碰撞性和弱碰撞性

**试比较对称加密，Hash函数和Mac消息鉴别码的区别和联系。**

**(从功能用途；构造方法上（对称可以构造hash和mac,hash可以构造mac）;安全性；密钥**

对称加密可以将任意长度明文通过密钥和加密算法转换成相应的密文，反向可逆，可用来构造hash函数和mac函数，hash函数用来认证和判断消息的完整性，是将任意长度明文通过它可以生成定长数据，不需要密钥，不可逆，叶可用来构造mac函数，mac函数使用密钥对明文产生定长的mac值，用来认证和保护数据的完整性。

**13数字签名和认证协议**

**数字签名**：

直接数字签名：

用自己的私钥来对整个消息或消息的散列值加密产生数字签名

缺点：发送方 抵赖自己从未发过，自己私钥丢失

可加：时间戳，但是在时刻T丢失，攻击者可以提供一个T之前的时间戳

仲裁数字签名：

可靠第三方，每次自己的数据先发给第三方，第三方来转发（如果不想让仲裁者看到自己的数据，就让xy双方的密钥进行一下加密，只让1仲裁者转发就可

对称加密算法（NS提出）

5步走以及其中产生的一些问题和需要解决的办法：（P279——P281）

数字签名必须具有下列特征：

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

签名应满足下列条件：

1. 签名必须是与消息相关的二进制位串（2）签名必须使用发送方某些独有的信息，以防伪造和否认（3）产生数字签名比较容易（4）验证和识别数字签名比较容易（5）伪造数字签名在计算上是不可行的，无论是从给定的数字签名伪造消息还是从给定的消息伪造数字签名在计算上都是不可行的（6）保存数字签名的拷贝是可行的

DSA需要掌握其特点图（P234）：

**14认证的实际运用：**

**Kerberos(背景，安全需求，协议的工作流程，对安全性有效性进行探讨)**

**基本原理：**

**认证协议是一种完全采用对称算法完成的分布式服务器和用户服务访问认证的技术协议。系统中设有一个保存所有用户口令的AS服务器以及TGS服务器，用户首先向AS服务器申请访问TGS服务器的授权票据，然后用户访问TGS服务器申请访问应用服务器，之后用户拿着TGS服务器发送的访问应用服务器的票据去访问相应的应用服务器，引用服务器还要发送一个时间戳来验证改用户是不是假冒的。**

要解决的问题

用户可以通过某种途径进入工作站的并假装是其他用户操作工作站

用户可以通过变更工作站的网络地址，从该机上发送伪造的请求

用户可以监听信息交换并使用重放攻击，以获得服务或破坏正常操作

使用假冒服务器从而骗的用户的机密信息

(1)简单的认证会话：

3步，一个票据：

两个问题：（1）每一次登录都需要去访问AS(认证服务器),容易造成单点失败问题（2）上述会话中，包含对口令的明文传输，网络且听者1可以不活，使用受害者的任何服务

(2)引入TGS（票据授权服务器）：每个用户仅一次的登录会话；每种服务类型仅一次，每次会话服务仅一次

5步，两个票据（简单进行了分层）

问题：通信的服务器V没有去验证C的身份

(3)对C进行一个简单的验证。（主要思想就是上层给下层分配想要让其解密的对象的ticket，解开就可以获得相应的内容）

其他一些相关概念的补充

**对称加密**

采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。

**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。会话密钥有时成对称密钥，因为同一密钥用于加密和解密。

**混合密码体制**

指用公钥密码加密一个用于对称加密的短期密码，再由这个短期密码在对称加密体制下加密实际需要安全传输的数据。

**非对称加密/公钥/私钥/证书/CA**

[对称加密算法](http://baike.sogou.com/lemma/ShowInnerLink.htm?lemmaId=453349&ss_c=ssc.citiao.link)在[加密和解密](http://baike.sogou.com/lemma/ShowInnerLink.htm?lemmaId=3855678&ss_c=ssc.citiao.link)时使用的是同一个秘钥；

而[非对称加密算法](http://baike.sogou.com/lemma/ShowInnerLink.htm?lemmaId=7513078&ss_c=ssc.citiao.link)需要两个[密钥](http://baike.sogou.com/lemma/ShowInnerLink.htm?lemmaId=267521&ss_c=ssc.citiao.link)来进行加密和解密，这两个秘钥公钥和私钥

**证书**

实际对于非对称加密算法（公钥加密）来说的，一般证书包括公钥、姓名、数字签名三ss个部分。证书好比身份证，证书机构（ca）就好比是公安局，职责就是负责管理用户的证书也就是身份证。

**CA**

是负责签发证书、认证证书、管理已颁发证书的机关。它要制定政策和具体步骤来验证、识别用户身份，并对用户证书进行签名，以确保证书持有者的身份和[公钥](http://baike.sogou.com/lemma/ShowInnerLink.htm?lemmaId=7882631&ss_c=ssc.citiao.link)的拥有权。网上的公众用户通过验证 CA 的签字从而信任 CA ，任何人都可以得到 CA 的证书（含公钥），用以验证它所签发的证书。

**分组算法**

将一个明文分组作为整体加密，得到等长的密文分组(64/128一组)，比流算法应用广泛

**流算法**

每次加密数据流的一位/一个字节 生成密钥->密钥流

**散列函数**：

输入是可变大小的消息M,输出是固定大小的散列码H(M),散列码并不使用密钥它仅仅是输入消息的函数，散列码也称为消息摘要

**S-Box（s盒）**

是密码学领域的一个基本组件，其功能是实现数据的非线性置换, 主要应用于对称加密算法中（DES\AES）

DES的盒是算法给出来的，没有计算依据，AES的S盒是计算出来的。

**IV**

DES中使用的初始向量，和密文具有相同长度的数据分组，必须收发方共享，但不能预测

**MD5** message digest 5

常用的一种hash函数之一，输出128bit，内部处理以512bit为单位，另一个常用的hash算法是SHA1.

**SHA1**

安全[哈希算法](http://baike.baidu.com/view/273836.htm)（Secure Hash Algorithm）主要适用于[数字签名](http://baike.baidu.com/view/7626.htm)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](http://baike.baidu.com/view/2396437.htm)。

**SHA2** SHA-224、SHA-256、SHA-384，和SHA-512并称为SHA-2。

新的散列函数并没有接受像SHA-1一样的公众密码社区做详细的检验，所以它们的密码安全性还不被大家广泛的信任。

虽然至今尚未出现对SHA-2有效的攻击，它的算法跟SHA-1基本上仍然相似；因此有些人开始发展其他替代的散列算法。

**MAC**

MAC认证技术，利用密钥生成一个固定长度的短数据块，并将该数据块附在消息之后，在这种方法中，AB共享密钥K，A计算MAC=C(K,M),B收到之后进行解密，看看M是否一样，来验证消息的完整性

**Diffie-Hellman Key Agreement Protocol：**

一种确保共享KEY安全穿越不安全网络的方法，它是OAKLEY的一个组成部分，是**建立密钥的**方法，不是加密方法，它巧妙在于需要安全通信的双方可以用这个方法确定对称密钥。

**离散对数问题**：

是包括Diffie-Hellman 密钥交换和数字签名算法（DSA）在内许多公钥算法的基础。对于方程  
y = g^x mod p，给定g、x、p可算出y，但是给定y、g、p计算x一般非常困难。(单向陷门函数)

ElGamal 密码体系：<https://blog.csdn.net/weixin_38134491/article/details/84542205>

分析

基于离散对数的公开密钥体制，它与Diffie-Hellman密钥分配体制密切相关。（电子版课本页码：218）

第八章：

费马小定理的证明+用途：（P169）

1. 可以用于素数测试miller-Rabin算法
2. 可以为RSA算法的正确性提供支持

欧拉定理证明（P171）

**几种攻击模式的简要介绍：**

**中间人攻击**

中间人攻击（Man-in-the-MiddleAttack，简称“MITM攻击”）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，这台计算机就称为“中间人”。

**生日攻击**

生日攻击方法没有利用Hash函数的结构和任何代数弱性质，它只依赖于消息摘要的长度，即Hash值的长度

* 最多尝试2n＋1个报文，必有至少一对碰撞
* 问：平均尝试多少个报文，可以以1/2的概率找到一对碰撞？

~ 2n/2

* 类比问题（生日问题）
  + 最多找365+1个人，则必有至少两个人生日相同
  + 问：平均找多少个人，能以1/2的概率找到两人生日相同？

23

**蛮力攻击（brute-force attack）**

也叫强行攻击，对所有可能的密钥进行尝试(穷举法)

**字典攻击**

在破解密码或密钥时，逐一尝试用户自定义词典中的可能密码（单词或短语）的攻击方式

**简答题：**

1. **对称算法DES/AES/RC4/3DES特点、安全特性与适用场合；**

DES：对称分组密码体制。密钥短，加密简单，速度快 在穷举攻击下较为脆弱 适用于大量加密数据

AES：对称分组密码体制 高级加密标准安全 适用场合广泛（数字签名 文档加密 商业领域）迟早代替DES算法

RC4:序列密码算法 速度快，但需要安全传递密钥 安全性比较高 应用于SSL和WEP协议

3DES：三重加密，比DES更安全，应用于更新DES的场景，使用2个或三个密钥。

实际3DES加密的过程式子：（P127）

加密k1-解密k2-加密k1

使用的密钥个数减少了，便于密钥的管理，而且安全性也没有丧失

1. **公钥算法的用途**

**加解密；数字签名；密钥交换（密钥分发(非对称)和密钥协商（kdc））**

**补充：diff-hellman只可以来密钥交换；DSS(数字加密标准)：只可以用来数字签名**

**4. Hash函数的特性与用途；**

文件校验 数字签名 挑战-认证

Hash函数常用来从口令产生密钥，签名前对消息hash取特征，在鉴别码中保护完整性，用来产生伪随机数，用作预防重放攻击的一次性值等，还有在系统文件防护和P2P共享方面，hash函数常用来唯一的标识一个文件。

1.RSA公钥算法

在RSA密码中关键是如何有效选取一个大素数，而在这个大素数的选取过程中，先必须产生一个大的随机的奇数，然后再来检验其是否为素数（探究其可行性）。否则继续选取。RSA的安全性主要就是***基于大数的分解***，因此，随机数的选取就显得尤为重要。

**7．MAC和对称算法都有密钥，为什么攻击MAC比攻击密钥更加困难？**

在对称算法中，只要获得一个密钥，就攻破了该加密，其函数体现的是一对一的关系，但是在MAC里面，是多对一的，得到一个随机数使得加密之后的消息一样，该随机数并不一定是真正的密钥，还需要去验证其他。

**8．对散列函数的要求**

H可应用于任意大小的数据块；产生定长的输出；计算H(M)比较容易实现，硬件和软件支持；单向函数；抗弱碰撞性；抗强碰撞性

**9：散列函数的几种构造方法：**

分组异或的值作为输出；增强（每处理完一个分组后，将散列值循环左移一位）；不仅对散列值加密，也对消息（CBC）加密

**10：认证和密钥交换使用两种方法来抵抗重放攻击**

时间戳；挑战、应答

**11：DSS中的DSA算法和RSA的比较：**

RSA:实验中的逻辑

DSS:散列码和为此次签名而产生的随机数k作为签名函数的书u，签名函数依赖于发送方的私钥和一组参数，可认为这组参数一起构成来全局公钥，签名由两部分构成，

DSA算法：建立在求离散对数的困难性

验证DSA算法的正确性和可靠性：

**12、one-time pad为什么才是真安全：**

一次一密(One-Time-Pad),用随机的非重复的字符集合作为输出密文.这里最重要的是,一旦使用了变换的输入密文,就不再在任何其他消息中使用这个输入密文(因此是一次性的).输入密文的长度等于原消息明文的长度.

**13、**

试卷中的简答题：

1. 简述计算安全和理论安全，并以此说明RSA,ONE\_TIME\_PAD的安全性

计算安全：破解的代价超出密文信息的价值；破译密码的时间超出密文的有效生命期

无条件安全：无论有多少可使用的密文，都不足以唯一的确定密文所对应明文的一次一密。

理论安全：

一次一密，密钥只对一个消息进行加解密，之后丢弃不用，每一条新的消息都需要一个与其等长的密钥，对于一个密文，给出任何一个与其等长的明文都可以找到一个密钥。

1. 说明公钥，私钥，证书，CA之间的联系，并说明私钥和证书之间的关系
2. 设计一种算法要求实现机密性，完整性和不可抵赖性，要求使用公钥算法，对称算法和Hash算法

（11）DES，AES,RC4，对比和适用场合，现代对称加密算法的趋势

（12）口令和密钥的关系，密钥分配常用哪些方法

（13）公钥证书体系的工作原理

（14）账号口令机制的改进，利用hash函数挑战应答方法

(15) 攻击类型：惟密文攻击；已知明文攻击；选择明文攻击；选择密文攻击；选择文本攻击；

（16）DES的构造步骤和方法：

I:IP初始置换；复杂算法fk,用k1子密钥对右半部分进行加密；左右再次进行置换；复杂算法fk(2轮),用k2子密钥对右半部分进行加密；IP’初始置换逆置换