A卷选择

1 属于对称算法和非对称算法的是

对称算法就是整个加密解密过程使用同一个密钥，并且可以密文-密钥反推出原文；而非对称算法采用了两个密钥.加密，一般是1的公钥加密，1的私钥解密

常见的对称算法：DES,3DES,IDEA,AES,SM1,SM4

常见的非对称算法：SM2,RSA,ECC

2数字签名解决篡改和伪造的问题

数字签名以及验证的流程为：

首先对于要传输的**原文**，使用HASH计算，可以得到**原文摘要**，然后本人使用**私钥**将原文摘要进行**加密**，此密文即为传输过程中的**签名**；

接收者收到传输数据后，需要对内容进行验证，查看内容是否为原文，是否被篡改，使用**公钥**对签名进行**解密**，得到**原文摘要**，然后自己在本地也对取得的**当前原文进行HASH计算**，得到**当前原文的摘要**，将解密得到的摘要与自己计算得到的摘要进行**比对**，查看是否一致即可验证。

3 PKI   67

4 数字证书不包含哪些信息  不包含个人私有秘钥

包含的信息有：版本号，序列号，签名算法标识，签发者，有效期，证书主体名，证书主体的公钥信息，签发者唯一标识，证书主体唯一标识，扩展，签名。

5 套接字  SSL协议位于哪一部分

SSL协议工作在应用层和传输层之间/Socket层，在网络协议层次上位于tcp/ip协议之上

6 和上一题有关

7 数字签名用的哪种方法

四个选项 ：身份认证 加密 传输数据 访问控制

正确 身份认证

8 生物认证里不适合作为认证特征的是

指纹，虹膜，DNA,都可以     身高体重不可以

9  防止重放攻击最有效的方法

错误 使用复杂的密码 经常修改用户名密码 对账户进行加密

正确  使用“一次一密”加密方式

10 计算机病毒的危害性表现在什么

破坏程序和数据

11 软件加密和硬件加密比较

速度：硬件比软件快

硬件安全性更好，更易于安装

大概率这个选项   兼容性：软件加密兼容性比硬件好

12 计算机网络中使用的加密方式有哪些种

点对点  链路 端对端

13 计算机病毒的特征

破坏性，传染性，隐蔽性，潜伏性，多态性，不可预见性

14  使用的防杀毒软件作用

所有 全部 绝对  都是错的    只能杀一部分

15 拒绝服务攻击

通过非法入侵控制  
16利用软件缺陷进行网络攻击最有效防范方法

打补丁

17 机器如果运行速度慢，CPU使用率高，判断受到攻击的方式

选项中有 木马  欺骗

正确    拒绝服务攻击 

18  木马病毒属于哪种类型       
蠕虫病毒  宏病毒  引导性病毒    
正确  基于CS结构的病毒             

19   有哪几种攻击方法  含义   145         
SYN泛洪攻击  UDP泛洪攻击   ping泛洪攻击   泪滴攻击  land攻击  smurf攻击

20  VPN定义

通过公用网络建立虚拟专用网络

A卷填空

填空  
1 网络安全属性 五个    
保密性 真实性 安全性 可控性 可用性

2 OSI五大类安全服务  
鉴别服务 访问控制服务 数据保密性服务 数据完整性服务 不可否认服务

3密码学发展的三个阶段

古典密码学 近代密码学 现代密码学

4 密码学分支   
密码编译学 密码编码学

5 消息鉴别系统构成  
  鉴别算法  鉴别协议 鉴别函数

6数字签名功能  
  防抵赖 防篡改 防伪造 防冒充

7 PKI信任模型  
 层次模型 交叉模型 混合模型 桥CA模型 信任链模型

8 IPSEc 工作模式  
传输模式  隧道模式

9 防火墙体系结构  三种  
单宿堡垒主机 双宿堡垒主机 屏蔽子网防火墙

10 VPN类型  
  “两层隧道  三层隧道”

两套卷的大题部分    
包含名词解释，简答题，大题  
1、VPN定义

即虚拟专用网络，在VPN客户机与VPN网关之间创建一个加密的、虚拟的点对点连接，保障数据在经过互联网时的安全。

2、数字证书定义

数字证书就是互联网通讯中标志通讯各方身份信息的一串数字，提供了一种在Internet上验证通信实体身份的方式，数字证书不是[数字身份证](https://baike.so.com/doc/6139609-26246096.html" \t "https://baike.so.com/doc/_blank)，而是身份认证机构盖在数字身份证上的一个章或印。

1. DES加密流程  比较复杂 几步需要知道 19  
   初始置换IP 16轮迭代 初始逆置换（IP -1次方）
2. 信息安全、计算机网络安全定义  
   信息安全：指信息系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，信息系统连续、可靠、正常地运行，信息服务不中断。

计算机网络安全：计算机及其网络系统资源和信息资源不受自然和人为有害因素的威胁和危害。

1. 数字签名定义

附加在数字单元上的一些数据、或是对数据单元所做的一些密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性，并保护数据，防止被人进行伪造

1. 防火墙定义  功能  特点

定义：由软件和硬件组合而成的、起过滤和封锁作用的计算机系统或者网络系统

功能：访问控制功能、内容控制功能、日志功能、集中管理功能

特点：1）所有的通信，无论是从内部到外部或者外部到内部，都必须经过防火墙。

1. 只有被授权的通信才能通过防火墙
2. 防火墙本身对于渗透必须是免疫的
3. RSA流程   简单描述一下

客户端需要加密时，先向服务端发起一个请求，请求RSA的公钥

服务端获取到请求之后，生成公钥，返回给客户端

客户端拿到公钥之后，使用公钥加密明文

客户端将公钥加密之后的密文发给服务器

服务端获取客户端密文，使用私钥解密可以得到明文

1. 入侵检测过程

信息收集、信息预处理、数据的检测分析、根据安全策略做出响应。

1. PGP提供的服务  五种  
   认证、机密性、压缩、电子邮件的兼容性、分段
2. 计算机病毒定义 特征

定义：人为编制的、能够对计算机正常程序的执行或数据文件造成破坏，并且能够自我复制的一种指令程序代码。

特征：破坏性、传染性、隐蔽性、潜伏性、多态性、不可预见性

1. 蜜罐技术

本质上是一种对攻击方进行欺骗的一种技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。 

1. 利用公钥实现数字签名 非对称方法 书上有图

假设接收方已知发送方的公钥，则发送方可以用自己的私钥对整个消息或消息的散列码加密来产生数字签名，接收方用发送方的公钥对签名进行验证从而确认签名和消息的真实性

13、隧道技术概念

通过使用互联网络的基础设施在网络之间传递数据的方式使用隧道传递的数据可以是不同协议的PDU，隧道将其他协议的PDU重新封装后通过网络发送，新的PDU提供路由信息，以便通过互联网传递被封装的数据。

1. 安全关联

在两个使用IPSec的实体间建立的逻辑连接，定义了实体问如何使用安全服务进行通信。

B卷选择  
1 置换和代换 判断是置换还是代换  
   置换：仅仅改变明文字母的位置

代换：将明文中字母用其他字母、数字或符号替换的一种方法

2 PKI 实现了什么功能

实现了：认证、完整性、加密 和权限没有关系

3 CA功能

主要是负责生成、发放、管理数字证书等

4 数字证书包含的内容

版本号，序列号，签名算法标识，签发者，有效期，证书主体名，证书主体的公钥信息，签发者唯一标识，证书主体唯一标识，扩展，签名。  
  
5 最安全的认证是哪一种形式  指纹  
   通过密钥 认证卡 验证码 指纹

6 ARP

ARP：地址解析协议，根据IP地址获取物理地址的一个TCP/IP协议。

ARP欺骗：冒充ARP地址

7 非对称典型代表

RSA

8 主动攻击 被动攻击 有哪些类型

主动攻击：具有破坏性，分为中断、篡改、伪造

被动攻击：不具有破坏性，分为被动的获取消息的内容，对业务数据流分析

9 清除病毒最有效的方法 选项有：杀毒、删数据、删文件

格式化

10 木马和病毒 区别  
   木马有潜伏性  病毒具有传染性

11 入侵检测系统步骤  
   收集信息 信息分析 结果处理（入侵）

12 Ping命令的攻击 属于什么方法 属于拒绝服务攻击的一种形式  
   不属于：篡改、重放 、冒充 抵赖

13 老师没说

14 数据完整性定义 指的是什么？

[存储](https://baike.so.com/doc/4223154-4424731.html)在数据库中的所有数据值均正确的状态。如果数据库中存储有不正确的数据值，则该数据库称为已丧失[数据](https://baike.so.com/doc/5387430-7565065.html)完整性。

15  Smurf攻击  ICMP泛洪 ping命令攻击 定义

Smurf攻击:通过向一个局域网的广播地址发出ICMP回应请求，并将请求的返回地址设为被攻击的目标主机，导致目标主机被大量的应答包淹没，最终导致目标主机崩溃。

ICMP泛洪:利用ICMP报文 进行攻击的一种方法。如果攻击者向目标主机发 送大量的ICMP ECHO报文，将产生ICMP泛洪， 目标主机会将大量的时间和资源用于处理ICMP ECHO报文，而无法处理正常的请求或响应，从而实现对目标主机的攻击。

Ping泛洪攻击：ICMP包规定最大尺寸64KB，加载的尺寸超过64KB，会出现内存分配错误，导致TCP/IP堆栈崩溃，致使接收方主机宕机。

16  防范口令攻击方法  不可以的是  
       用防火墙

17 生物认证里不适合作为认证特征的是

指纹，虹膜，DNA,都可以     身高体重不可以  
  
18 19 20 计算机病毒的危害性  特征  定义  类型  
 特征：破坏性、传染性、隐蔽性、潜伏性、多态性、不可预见性

定义：人为编制的、能够对计算机正常程序的执行或数据文件造成破坏，并且能够自我复制的一组指令程序代码。

类型：良性病毒和恶性病毒；文件型病毒和引导型病毒；

危害性：破坏计算机数据、占用计算机空间、破坏计算机硬盘。

填空  
1信息安全的属性  
  机密性 完整性  真实性   
  可用性  可控性    
2    五大安全的策略  
物理安全策略、访问控制策略、防火墙控制、信息加密策略、网络安全管理策略  
3 密码体制有哪几部分组成  
  明文 密文 密钥 加密算法 解密算法  
4 古典密码体制中两种传统加密基本技巧  
  置换  代换  
5 身份认证保证   和   的统一  
   物理身份  数字身份  
6 IPSEC协议体系结构 五大部分组成  
ESP协议  AH协议 密钥管理 加密算法 认证算法  
7 计算机病毒按照传染方式分为哪几种  
   文件型  引导型  混合型  
8 未知 应该和计算机病毒有关 如特征、定义、类型  
9 未知 应该和计算机病毒有关  
10 入侵检测过程  
  信息收集  信息分析  结果处理

判断题

信息安全和网络安全实际上是殊途同归的关系   对  
计算机网络中单独的一层可以提供全部的安全属性   错  
密码学是研究密码编码分析的  对  
数字签名解决数字加密    错  
CN负责证书的颁发，管理   对  
Kerberos认证协议是一种对称的、双向性的  对  
IPSec协议是独立于鉴别和加密算法的，在一定框架中可以使用不同的鉴别和加密方式 对

IPSec协议是介于网络层和传输层之间的安全套接层协议 错

SSL协议在传输层和应用层之间 对

第九个 VPN检测系统。。技术 对

第十个 VPN既能认证，也能加密 对

隧道定义

隧道。。封装的系统 包含互联网传递。。 对