**李晓君 网络安全**

1.[单选题]计算机网络安全是指利用计算机网络管理控制和技术措施，保证在网络环境中数据的（ ）、完整性、网络服务可用性和可审查性收到保护。

**A.保密性**

B.抗攻击性

C.网络服务管理性

D.控制安全性

正确答案：A

2.[单选题]网络安全的实质和关键是保护网络的（ ）安全。

A.系统

B.软件

**C.信息**

D.网站

正确答案：C

3.[单选题]实际上，网络的安全包括两大方面的内容，一是（ ），二是网络的信息安全。

A.网络安全服务

**B.网络的系统安全**

C.网络设备安全

D.网络环境安全

正确答案：B

4.[单选题]下面不属于TCSEC标准定义的系统安全等级的4个方面是( )。

A.安全政策

B.可说明性

C.安全保障

D.安全特征

正确答案：D

5.[单选题]在短时间内向网络中的某台服务器发送大量无效连接请求，导致合法用户暂时无法访问服务器的攻击行为是破坏了( )。

A.机密性

B.完整性

C.可用性

D.可控性

正确答案：C

6.[单选题]如果访问者有意避开系统的访问控制机制，则该访问者对网络设备及资源进行非正常使用属于( )。

A.破环数据完整性

B.非授权访问

C.信息泄漏

D.拒绝服务攻击

正确答案：B

7.[单选题]实体安全包括（ ）。

A.环境安全和设备安全

B.环境安全、设备安全和媒体安全

C.物理安全和环境安全

D.其他方面

正确答案：B

8.[单选题]在网络安全中，常用的关键技术可以归纳为（ ）三大类。

A.计划、检测、防范

B.规划、监督、组织

C.检测、防范、监督

D.预防保护、检测跟踪、响应恢复

正确答案：D

9.[填空题]计算机网络安全是一门涉及 \_\_\_\_、\_\_\_\_、\_\_\_\_、通信技术、应用数学、密码技术、信息论等多学科的综合性学科。

正确答案:

(1) 计算机科学

(2) 网络技术

(3) 信息安全技术

10.[填空题]网络安全的5 大要素和技术特征，分别是 \_\_\_\_、\_\_\_\_、\_\_\_\_、\_\_\_\_、\_\_\_\_。

正确答案:

(1) 机密性

(2) 完整性

(3) 可用性

(4) 可控性

(5) 不可否认性

11.[填空题]计算机网络安全所涉及的内容包括是\_\_\_\_、\_\_\_\_、\_\_\_\_、\_\_\_\_、\_\_\_\_等五个方面。

正确答案:

(1) 实体安全

(2) 运行安全

(3) 系统安全

(4) 应用安全

(5) 管理安全

12.[填空题]网络信息安全保障包括\_\_\_\_、\_\_\_\_、\_\_\_\_和\_\_\_\_四个方面。

正确答案:

(1) 信息安全策略

(2) 信息安全管理

(3) 信息安全运作

(4) 信息安全技术

1.[单选题]根据《网络安全法》的规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在( )。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估，法律、行政法规另有规定的，依照其规定。

A.境外存储B.外部存储器储存C.第三方存储D.境内存储

正确答案：D

2.[单选题]国家鼓励开发网络数据安全保护和利用技术，促进( )开放，推动技术创新和经济社会发展。

A.公共图书馆资源B.国家数据资源C.公共学校资源D.公共数据资源

正确答案：D

3.[单选题]国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的( )和水平，形成全社会共同参与促进网络安全的良好环境。

A.网络安全意识B.网络诚信意识C.网络社会道德意识D.网络健康意识

正确答案：A

4.[单选题]根据《网络安全法》的规定，国家实行网络安全( )保护制度。

A.等级B.分层C.结构D.行政级别

正确答案：A

5.[单选题]《网络安全法》规定，各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并( )有关单位做好网络安全宣传教育工作。

A.指导、督促B.支持、指导C.鼓励、引导D.支持、引导

正确答案：A

6.[单选题]国家建立和完善网络安全标准体系。( )和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

A.电信研究机构B.国务院标准化行政主管部门C.网信部门D.电信企业

正确答案：B

7.[单选题]网络产品、服务的提供者不得设置( )，发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

A.恶意程序B.风险程序C.病毒程序D.攻击程序

正确答案：A

8.[单选题]国家推进网络安全( )建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

A.社会化识别体系B.社会化评估体系C.社会化服务体系D.社会化认证体系

正确答案：C

9.[单选题]根据《网络安全法》的规定，( )负责统筹协调网络安全工作和相关监督管理工作。

A.中国电信B.信息部C.国家网信部门D.中国联通

正确答案：C

10.[单选题]根据《网络安全法》的规定，( )应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

A.电信科研机构

B.电信企业

C.网络合作商

D.网络运营者

正确答案：D

11.[单选题]网络产品、服务具有( )的，其提供者应当向用户明示并取得同意，涉及用户个人信息的，还应当遵守《网络安全法》和有关法律、行政法规关于个人信息保护的规定。

A.公开用户资料功能

B.收集用户信息功能

C.提供用户家庭信息功能

D.用户填写信息功能

正确答案：B

12.[单选题]国家实施网络( )战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

A.信誉身份B.可信身份C.安全身份D.认证身份

正确答案：B

13.[单选题]网络产品、服务应当符合相关国家标准的( )要求。

A.自觉性B.规范性C.建议性D.强制性

正确答案：D

14.[单选题]网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构( )或者安全检测符合要求后，方可销售或者提供。

A.认证设备合格

B.安全认证合格

C.认证网速合格

D.认证产品合格

正确答案：B

15.[单选题]关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的( )。

A.国家采购审查

B.国家网信安全审查

C.国家安全审查

D.国家网络审查

正确答案：C

16.[单选题]关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险( )至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

A.四年B.两年C.每年D.三年

正确答案：C

17.[单选题]国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事( )的活动，为未成年人提供安全、健康的网络环境。

A.针对未成年人黄赌毒

B.灌输未成年人错误网络思想

C.侵害未成年人受教育权

D.危害未成年人身心健康

正确答案：D

18.[单选题]国家( )关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

A.投资B.引导C.鼓励D.支持

正确答案：C

19.[单选题]网络相关行业组织按照章程，( )，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

A.提升行业标准B.宣传行业规范C.加强行业自律D.遵守行业规范

正确答案：C

20.[单选题]关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订( )，明确安全和保密义务与责任。

A.保密合同B.安全服务合同C.安全保密协议D.安全责任条款

正确答案：C

21.[多选题]《网络安全法》所称网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行( )的系统。

A.存储B.传输、交换C.处理D.收集

正确答案：ABCD

22.[多选题]国家支持网络运营者之间在网络安全信息( )等方面进行合作，提高网络运营者的安全保障能力。

A.分析B.通报C.应急处置D.收集

正确答案：ABCD

23.[多选题]根据《网络安全法》的规定，国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，( )。

A.支持企业、研究机构和高等学校等参与国家网络安全技术创新项目

B.支持网络安全技术的研究开发和应用

C.推广安全可信的网络产品和服务

D.保护网络技术知识产权

正确答案：ABCD

24.[多选题]建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施( )。

A.同步修改B.同步使用C.同步建设D.同步规划

正确答案：BCD

25.[多选题]国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害( )的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

A.公共利益B.网速C.国计民生D.国家安全

正确答案：ACD

26.[多选题]网络运营者应当制定网络安全事件应急预案，及时处置( )安全风险，在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

A.系统漏洞B.网络攻击C.网络侵入D.计算机病毒

正确答案：ABCD

27.[多选题]国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列( )措施。

A.对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助

B.促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享

C.对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估

D.定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力

正确答案：ABCD

28.[多选题]根据《网络安全法》的规定，任何个人和组织( )。

A.不得从事非法侵入他人网络、干扰他人网络正常功能等危害网络安全的活动

B.不得提供专门用于从事侵入网络、干扰网络正常功能等危害网络安全活动的程序

C.明知他人从事危害网络安全的活动的，不得为其提供技术支持

D.明知他人从事危害网络安全的活动的，可以为其进行广告推广

正确答案：ABC

29.[多选题]国家支持( )等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

A.中小学校B.职业学校C.高等学校D.企业

正确答案：BCD

30.[多选题]网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列( )措施。

A.要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测

B.向社会发布网络安全风险预警，发布避免、减轻危害的措施

C.组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度

D.要求单位和个人协助抓跑嫌犯

正确答案：ABC

31.[多选题]网络运营者收集、使用个人信息，应当遵循( )的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

A.公平B.正当C.合法D.必要

正确答案：BCD

32.[多选题]任何个人和组织应当对其使用网络的行为负责，不得设立用于( )等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

A.实施诈骗B.制作或者销售违禁物品C.制作或者销售管制物品D.传授犯罪方法

正确答案：ABCD

33.[多选题]根据《网络安全法》的规定，关键信息基础设施的运营者应当履行( )安全保护义务。

A.设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查

B.对重要系统和数据库进行容灾备份

C.制定网络安全事件应急预案，并定期进行演练

D.定期对从业人员进行网络安全教育、技术培训和技能考核

正确答案：ABCD

34.[多选题]网络运营者不得( )其收集的个人信息，未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

A.泄露B.使用C.毁损D.篡改

正确答案：ACD

35.[多选题]网络运营者违反《网络安全法》的规定，有下列行为( )之一的，由有关主管部门责令改正，拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款。

A.不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的

B.拒不向公安机关、国家安全机关提供技术支持和协助的

C.拒绝、阻碍有关部门依法实施的监督检查的

D.拒不向配合公安机关提供技术密码的

正确答案：ABC

36.[多选题]《网络安全法》所称网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的( )的能力。

A.可用性B.完整性C.保密性D.真实性

正确答案：ABC

37.[多选题]网络运营者为用户( )，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

A.办理网络接入、域名注册服务

B.办理固定电话、移动电话等入网手续

C.办理监听业务

D.为用户提供信息发布、即时通讯等服务

正确答案：ABD

38.[多选题]根据《网络安全法》的规定，有下列( )行为之一的，由有关主管部门责令改正，给予警告，拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

A.擅自终止为其产品、服务提供安全维护的

B.未按照规定及时告知用户并向有关主管部门报告的

C.设置恶意程序的

D.对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施的

正确答案：ABCD

39.[多选题]网络运营者应当按照网络安全等级保护制度的要求，履行( )安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

A.采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施

B.制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任

C.采取数据分类、重要数据备份和加密等措施

D.采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月

正确答案：ABCD

40.[多选题]境外的机构、组织、个人从事( )等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

A.攻击B.干扰C.侵入D.破坏

正确答案：ABCD

41.[判断题]国家机关政务网络的运营者不履行《网络安全法》规定的网络安全保护义务的，由其同级机关或者有关机关责令改正，对直接负责的主管人员和其他直接责任人员依法给予处分。

A.对

B.错

正确答案：错

42.[判断题]国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

A.对

B.错

正确答案：对

43.[判断题]存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守《网络安全法》外，还应当遵守保密法律、行政法规的规定。

A.对

B.错

正确答案：对

44.[判断题]根据《网络安全法》的规定，市级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

A.对

B.错

正确答案：错

45.[判断题]根据《网络安全法》的规定，有关部门可以对举报人的相关信息予以保密，保护举报人的合法权益。

A.对

B.错

正确答案：错

46.[判断题]任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益的活动。

A.对

B.错

正确答案：对

47.[判断题]根据《网络安全法》的规定，大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

A.对

B.错

正确答案：对

48.[判断题]国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

A.对

B.错

正确答案：对

49.[判断题]网信部门和有关部门在履行网络安全保护职责中获取的信息，用于维护网络安全的需要，也可以用于其他用途。

A.对

B.错

正确答案：错

50.[判断题]网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

A.对

B.错

正确答案：对

1.[单选题]SSL协议是( )之间实现加密传输的协议。

A.物理层和网络层

B.网络层和系统层

C.传输层和应用层

D.物理层和数据层

正确答案：C

2.[单选题]加密安全机制提供了数据的( )。

A.可靠性和安全性

B.保密性和可控性

C.完整性和安全性

D.保密性和完整性

正确答案：D

3.[单选题]抗抵赖性服务对证明信息的管理与具体服务项目和公证机制密切相关，通常都建立在( )层之上。

A.物理层

B.网络层

C.传输层

D.应用层

正确答案：D

4.[单选题]能在物理层、链路层、网络层、传输层和应用层提供的网络安全服务的是( )。

A.认证服务

B.数据保密性服务

C.数据完整性服务

D.访问控制服务

正确答案：B

5.[单选题]传输层由于可以提供真正的端到端的连接，最适宜提供( )安全服务。

A.数据保密性及以上各项

B.数据完整性

C.访问控制服务

D.认证服务

正确答案：A

6.[填空题]应用层安全分解成\_\_\_\_、\_\_\_\_、\_\_\_\_安全，利用各种协议运行和管理。

正确答案:

(1) 网络层

(2) 操作系统

(3) 数据库

7.[填空题]安全套层SSL协议是在网络传输过程中，提供通信双方网络信息\_\_\_\_ 和\_\_\_\_，由\_\_\_\_和\_\_\_\_两层组成。

正确答案:

(1) 保密性

(2) 可靠性

(3) SSL协商层

(4) 记录层

8.[填空题]ISO对OSI规定了\_\_\_\_、\_\_\_\_、\_\_\_\_、\_\_\_\_、\_\_\_\_五种级别的安全服务。

正确答案:

(1) 对象认证

(2) 访问控制

(3) 数据保密性

(4) 数据完整性

(5) 防抵赖

1.[单选题]计算机网络安全管理主要功能不包括( )。

A.性能和配置管理功能

B.安全和计费管理功能

C.故障管理功能

D.网络规划和网络管理者的管理功能

正确答案：D

2.[单选题]网络安全管理技术涉及网络安全技术和管理的很多方面，从广义的范围来看( )是安全网络管理的一种手段。

A.扫描和评估

B.防火墙和入侵检测系统安全设备

C.监控和审计

D.防火墙及杀毒软件

正确答案：B

3.[单选题]名字服务、事务服务、时间服务和安全性服务是( )提供的服务。

A.远程IT管理的整合式应用管理技术

B.APM网络安全管理技术

C.CORBA网络安全管理技术

D.基于WeB的网络管理模式

正确答案：C

4.[单选题]与安全有关的事件，如企业猜测密码、使用未经授权的权限访问、修改应用软件以及系统软件等属于安全实施的( )。

A.信息和软件的安全存储

B.安装入侵检测系统并监视

C.对网络系统及时安装最新补丁软件

D.启动系统事件日志

正确答案：D

5.[单选题]( )功能是使用户能够过轮询、设置关键字和监视网络事件来达到网络管理目的，并且已经发展成为各种网络及网络设备的网络管理协议标准。

A.TCP/IP协议

B.公共管理信息协议CMIS/CMIP

C.简单网络管理协议SNMP

D.用户数据报文协议UDP

正确答案：C

6.[单选题]网络安全保障体系框架的外围是（ ）。

A.风险管理

B.法律法规

C.标准的符合性

D.上述三点

正确答案：D

7.[单选题]我国网络安全立法体系框架分为（ ）。

A.构建法律、地方性法规和行政规范

B.法律、行政法规和地方性法规、规章、规范性文档

C.法律、行政法规和地方性法规

D.以上都不对

正确答案：B

8.[填空题]网络安全策略包括3个重要组成部分： 、 、 。

正确答案:

(1) 安全立法

(2) 安全管理

(3) 安全技术

9.[填空题]网络安全保障包括 、 、 和 四个方面。

正确答案:

(1) 信息安全策略

(2) 信息安全管理

(3) 信息安全运作

(4) 信息安全技术

1.[单选题]在黑客攻击技术中，( )是黑客发现获得主机信息的一种最佳途径。

A.网络监听

B.缓冲区溢出

C.端口扫描

D.口令破解

正确答案：C

2.[单选题]一般情况下，大多数监听工具不能够分析的协议是( )。

A.标准以太网

B.TCP/IP

C.SNMP和CMIS

D.IPX和DECNet

正确答案：C

3.[单选题]改变路由信息、修改WinDows NT注册表等行为属于拒绝服务攻击的( )方式。

A.资源消耗型

B.配置修改型

C.服务利用型

D.物理破坏型

正确答案：B

4.[单选题]( )是建立完善的访问控制策略，及时发现网络遭受攻击情况并加以追踪和防范，避免对网络造成更大损失。

A.动态站点监控

B.实施存取控制

C.安全管理检测

D.完善服务器系统安全性能

正确答案：A

5.[单选题]( )利用以太网的特点，将设备网卡设置为“混杂模式”，从而能够接收到整个以太网内的网络数据信息。

A.缓冲区溢出攻击

B.木马程序

C.嗅探程序

D.拒绝服务攻击

正确答案：C

6.[单选题]字典攻击被用于（ ）。

A.用户欺骗

B.远程登录

C.网络嗅探

D.破解密码

正确答案：D

7.[填空题]黑客的“攻击五部曲”是\_\_\_\_、\_\_\_\_、\_\_\_\_、\_\_\_\_、\_\_\_\_。

正确答案:

(1) 隐藏IP

(2) 踩点扫描

(3) 获得特权

(4) 种植后门

(5) 隐身退出

8.[填空题]端口扫描的防范也称为\_\_\_\_，主要有\_\_\_\_和\_\_\_\_两种方法。

正确答案:

(1) 系统加固

(2) 关闭闲置及危险端口

(3) 屏蔽出现扫描症状的端口

9.[填空题]密码攻击一般有\_\_\_\_、\_\_\_\_和\_\_\_\_三种方法。其中\_\_\_\_有蛮力攻击和字典攻击两种方式。

正确答案:

(1) 网络监听非法得到用户密码

(2) 密码破解

(3) 放置特洛伊木马程序

(4) 密码破解

10.[填空题] 就是利用更多的傀儡机对目标发起进攻，以比从前更大的规模进攻受害者。

正确答案:

(1) 分布式拒绝服务攻击（DDOS）

11.[填空题]按数据来源和系统结构分类，入侵检测系统分为3类，即 、 和 。

正确答案:

(1) 基于主机

(2) 基于网络

(3) 混合型

1.[单选题]( )密码体制，不但具有保密功能，并且具有鉴别的功能。

A.对称

B.私钥

C.非对称

D.混合加密体制

正确答案：C

2.[单选题]网络加密方式的( )是把网络上传输的数据报文的每一位进行加密，而且把路由信息、校验和等控制信息全部加密。

A.链路加密

B.节点对节点加密

C.端对端加密

D.混合加密

正确答案：A

3.[单选题]恺撒密码是( )方法，被称为循环移位密码，优点是密钥简单易记，缺点是安全性较差。

A.代码加密

B.替换加密

C.变位加密

D.一次性加密

正确答案：B

4.[单选题]在加密服务中，( )是用于保障数据的真实性和完整性的，目前主要有两种生成MAC的方式。

A.加密和解密

B.数字签名

C.密钥安置

D.消息认证码

正确答案：D

5.[单选题]根据信息隐藏的技术要求和目的，下列( )不属于数字水印需要达到的基本特征。

A.隐藏性

B.安全性

C.完整性

D.强壮性

正确答案：C

6.[单选题]使用密码技术不仅可以保证信息的（ ），还可以保证信息的完整性和准确性，防止信息被篡改、伪造和假冒。

A.保密性

B.抗攻击性

C.网络服务正确性

D.控制安全性

正确答案：A

7.[填空题]在加密系统中，原有的信息称为\_\_\_\_，由\_\_\_\_变为\_\_\_\_的过程称为加密，由\_\_\_\_还原成\_\_\_\_的过程称为解密。

正确答案:

(1) 明文

(2) 明文

(3) 密文

(4) 密文

(5) 明文

8.[填空题]\_\_\_\_是保护大型传输网络系统上各种信息的惟一实现手段，是保障信息安全的\_\_\_\_。

正确答案:

(1) 密码技术

(2) 核心技术

9.[填空题]对称密码体制加密解密使用\_\_\_\_的密钥;非对称密码体制的加密解密使用\_\_\_\_的密钥，而且加密密钥和解密密钥要求\_\_\_\_互相推算。

正确答案:

(1) 相同

(2) 不同

(3) 无法

10.[填空题]数据加密标准DES是\_\_\_\_加密技术，专为\_\_\_\_编码数据设计的，典型的按\_\_\_\_方式工作的\_\_\_\_密码算法。

正确答案:

(1) 代码加密

(2) 替换加密

(3) 变位加密

(4) 一次性加密

1.[单选题]在常用的身份认证方式中，( )是采用软硬件相结合、一次一密的强双因子认证模式，具有安全性、移动性和使用的方便性。

A.智能卡认证

B.动态令牌认证

C.USB Key

D.用户名及密码方式认证

正确答案：C

2.[单选题]以下( )属于生物识别中的次级生物识别技术。

A.网膜识别

B.DNA

C.语音识别

D.指纹识别

正确答案：C

3.[单选题]数据签名的( )功能是指签名可以证明是签字者而不是其他人在文件上签字。

A.签名不可伪造

B.签名不可变更

C.签名不可抵赖

D.签名是可信的

正确答案：A

4.[单选题]在综合访问控制策略中，系统管理员权限、读/写权限、修改权限属于( )。

A.网络的权限控制

B.属性安全控制

C.网络服务安全控制

D.目录级安全控制

正确答案：D

5.[单选题]以下( )不属于AAA系统提供的服务类型。

A.认证

B.鉴权

C.访问

D.审计

正确答案：C

6.[单选题]网络准入控制的基础是（ ）。

A.身份认证

B.数字签名

C.安全审计

D.数字证书

正确答案：A

7.[单选题]在我国的计算机系统安全保护等级划分中，系统审计保护级属于（ ）。

A.第一级

B.第二级

C.第三级

D.第四级

正确答案：B

8.[填空题]身份认证是计算机网络系统的用户在进入系统或访问不同\_\_\_\_的系统资源时，系统确认该用户的身份是否\_\_\_\_、\_\_\_\_和\_\_\_\_的过程。

正确答案:

(1) 保护级别

(2) 真实

(3) 合法

(4) 唯一

9.[填空题]数字签名是指用户用自己的\_\_\_\_对原始数据进行\_\_\_\_所得到\_\_\_\_，专门用于保证信息来源的\_\_\_\_、数据传输的\_\_\_\_和\_\_\_\_。

正确答案:

(1) 私钥

(2) 加密

(3) 特殊数字串

(4) 真实性

(5) 完整性

(6) 抗抵赖性

10.[填空题]访问控制包括三个要素，即\_\_\_\_、\_\_\_\_和\_\_\_\_。访问控制的主要内容包括\_\_\_\_、\_\_\_\_和\_\_\_\_三个方面。

正确答案:

(1) 主体

(2) 客体

(3) 控制策略

(4) 认证

(5) 控制策略实现

(6) 审计

11.[填空题]访问控制模式有三种模式，即 \_\_\_\_、\_\_\_\_和 \_\_\_\_。

正确答案:

(1) 自主访问控制DAC

(2) 强制访问控制MAC

(3) 基本角色的访问控制RBAC

1.[单选题]在计算机病毒发展过程中，( )给计算机病毒带来了第一次流行高峰，同时病毒具有了自我保护的功能。

A.多态性病毒阶段

B.网络病毒阶段

C.混合型病毒阶段

D.主动攻击型病毒

正确答案：C

2.[单选题]以病毒攻击的不同操作系统分类中，( )已经取代DOS系统，成为病毒攻击的主要对象。

A.UNIX系统

B.OS/2系统

C.Windows系统

D.NetWAre系统

正确答案：C

3.[单选题]( ) 是一种更具破坏力的恶意代码，能够感染多种计算机系统，其传播之快、影响范围之广、破坏力之强都是空前的。

A.特洛伊木马

B.CIH病毒

C.CoDeReDII双型病毒

D.蠕虫病毒

正确答案：D

4.[单选题]按照计算机病毒的链接方式不同分类，( )是将其自身包围在合法的主程序四周，对原来的程序不做修改。

A.源码型病毒

B.外壳型病毒

C.嵌入型病毒

D.操作系统型病毒

正确答案：B

5.[单选题]

计算机病毒的主要特点不包括（ ）。

A.潜伏性

B.破坏性

C.传染性

D.完整性

正确答案：D

6.[单选题]熊猫烧香是一种（ ）。

A.游戏

B.软件

C.蠕虫病毒

D.网站

正确答案：C

7.[单选题]木马的清除方式有手动清除和（ ）两种。

A.自动清除

B.手动清除

C.杀毒软件清除

D.不用清除

正确答案：C

8.[单选题]计算机病毒是能够破坏计算机正常工作的、（ ）的一组计算机指令或程序。

A.系统自带

B.人为编制

C.机器编制

D.不清楚

正确答案：B

9.[单选题]强制安装和难以卸载的软件都属于（ ）。

A.病毒

B.木马

C.蠕虫

D.恶意软件

正确答案：D

1.[单选题]拒绝服务攻击的一个基本思想是( )

A.向工作站不断发送垃圾邮件

B.迫使服务器的缓冲区满

C.迫使工作站和服务器停止工作

D.迫使服务器停止工作

正确答案：C

2.[单选题]TCP采用三次握手形式建立连接，在( )时候开始发送数据。

A.第一步

B.第二步

C.第三步之后

D.第三步

正确答案：C

3.[单选题]驻留在多个网络设备上的程序在短时间内产生大量的请求信息冲击某web服务器，导致该服务器不堪重负，无法正常相应其他合法用户的请求，这属于( )

A.上网冲浪

B.中间人攻击

C.DDoS攻击

D.MAC攻击

正确答案：C

4.[单选题]关于防火墙，以下( )说法是错误的。

A.防火墙能隐藏内部IP地址

B.防火墙能控制进出内网的信息流向和信息包

C.防火墙能提供VPN功能

D.防火墙能阻止来自内部的威胁

正确答案：D

5.[单选题]以下说法正确的是( )

A.防火墙能够抵御一切网络攻击

B.防火墙是一种主动安全策略执行设备

C.防火墙本身不需要提供防护

D.防火墙如果配置不当，会导致更大的安全风险

正确答案：D

6.[填空题]防火墙隔离了内部、外部网络，是内、外部网络通信的\_\_\_\_途径，能够根据制定的访问规则对流经它的信息进行监控和审查，从而保护内部网络不受外界的非法访问和攻击。

正确答案:

(1) 唯一

7.[填空题]防火墙是一种\_\_\_\_设备，即对于新的未知攻击或者策略配置有误，防火墙就无能为力了。

正确答案:

(1) 被动

8.[填空题]从防火墙的软、硬件形式来分的话，防火墙可以分为\_\_\_\_防火墙和硬件防火墙以及\_\_\_\_防火墙。

正确答案:

(1) 软件

(2) 芯片级

9.[填空题]包过滤型防火墙工作在OSI网络参考模型的\_\_\_\_和\_\_\_\_。

正确答案:

(1) 网络层

(2) 传输层

10.[填空题]第一代应用网关型防火墙的核心技术是\_\_\_\_。

正确答案:

(1) 代理技术

11.[填空题]单一主机防火墙独立于其它网络设备，它位于\_\_\_\_。

正确答案:

(1) 网络边界

12.[填空题] 是位于外围网络中的服务器，向内部和外部用户提供服务。

正确答案:

(1) 堡垒主机

13.[填空题] 利用TCP协议的设计上的缺陷，通过特定方式发送大量的TCP请求从而导致受攻击方CPU超负荷或内存不足的一种攻击方式。

正确答案:

(1) 拒绝服务攻击

1.[单选题]应对操作系统安全漏洞的基本方法不包括下面的( )

A.对默认安装进行必要的调整

B.给所有用户设置严格的口令

C.及时安装最新的安全补丁

D.更换到另一种操作系统

正确答案：D

2.[单选题]严格的口令策略不应当包含的要素是 ( )

A.满足一定的长度，比如8位以上

B.同时包含数字，字母和特殊字符

C.系统强制要求定期更改口令

D.用户可以设置空口令

正确答案：D

3.[单选题]恶意软件保护包括两部分内容( )

A.病毒防护和windows defender

B.病毒防护和实时保护

C.WINDOWS DEFENDER和实时保护

D.Windows Defender和扫描选项

正确答案：A

4.[单选题]范围广或异常的恶意程序，与病毒或蠕虫类似，会对用户的隐私和计算机安全造成负面影响，并损害计算机，这种警告登记属于( )

A.严重

B.高

C.中

D.低

正确答案：A

5.[单选题]如果软件试图更改重要的 Windows 设置，也会发出警报。由于软件已在计算机上运行，因此可以选择下列操作之一( )

A.隔离

B.删除

C.始终允许

D.许可

正确答案：A

6.[单选题]允许用户使用计算机的大多数功能，但是如果要进行的更改会影响计算机的其他用户或安全，则需要管理员的许可，属于什么帐户?( )

A.标准

B.管理员

C.来宾

D.贵宾

正确答案：A

1.[单选题]一个网络信息系统最重要的资源是 。

A.计算机硬件

B.网络设备

C.数据库

D.数据库管理系统

正确答案：C

2.[单选题]不应拒绝授权用户对数据库的正常操作，同时保证系统的运行效率并提供用户友好的人机交互指的是数据库系统的 。

A.保密性

B.可用性

C.完整性

D.并发性

正确答案：B

3.[单选题]数据库安全可分为两类:系统安全性和 。

A.数据安全性

B.应用安全性

C.网络安全性

D.数据库安全性

正确答案：A

4.[单选题]下面哪一项不属于Oracle数据库的存取控制: 。

A.用户鉴别

B.用户的表空间设置和定额

C.用户资源限制和环境文件

D.特权

正确答案：D

5.[单选题]（ ）是防止合法用户使用数据库时向数据库中加入不符合语义的数据。

A.安全性

B.完整性

C.并发性

D.可用性

正确答案：B

6.[单选题]下面不是由并发操作带来的数据现象是（ ）。

A.丢失更新

B.读“脏”数据(脏读)

C.违反数据约束

D.不可重复读

正确答案：C

7.[单选题]下载数据库数据文件，然后攻击者就可以打开这个数据文件得到内部的用户和帐号以及其它有用的信息，这种攻击称为（ ）。

A.对SQL的突破

B.突破script的限制

C.数据库的利用

D.对本地数据库的攻击

正确答案：D

8.[单选题]只备份上次备份以后有变化的数据，这样的数据备份类型是（ ）。

A.增量备份

B.差分备份

C.完全备份

D.按需备份

正确答案：A

9.[单选题]由非预期的、不正常的程序结束所造成的故障是（ ）。

A.系统故障

B.网络故障

C.事务故障

D.介质故障

正确答案：C

10.[单选题]权限管理属于下面哪种安全性策略（ ）。

A.系统安全性策略

B.用户安全性策略

C.数据库管理者安全性策略

D.应用程序开发者的安全性策略

正确答案：B

1.[单选题]对影响业务的故障，有应急预案的要求在( )之内完成预案的启动。

A.10分钟

B.15分钟

C.20分钟

D.30分钟

正确答案：D

2.[单选题]一般的防火墙不能实现以下哪项功能( )。

A.隔离公司网络和不可信的网络

B.防止病毒和特络依木马程序

C.隔离内网

D.提供对单点的监控

正确答案：B

3.[单选题]关闭系统多余的服务有什么安全方面的好处( )。

A.使黑客选择攻击的余地更小

B.关闭多余的服务以节省系统资源

C.使系统进程信息简单，易于管理

D.没有任何好处

正确答案：A

4.[单选题]在下列4 项中，不属于计算机病毒特征的是( )。

A.潜伏性

B.传染性

C.隐蔽性

D.规则性

正确答案：D

5.[单选题]对于重大安全事件按重大事件处理流程进行解决。出现重大安全事件，必须在( )分钟内上报省公司安全领导小组。迅速组织厂商、安全顾问公司人员现场抢修。

A.30

B.45

C.60

D.15

正确答案：A

6.[单选题]风险评估包括以下哪些部分( )

A.资产评估

B.脆弱性评估

C.威胁评估

D.以上都是

正确答案：D

7.[单选题]TCP SYN Flood网络攻击是利用了TCP建立连接过程需要( )次握手的特点而完成对目标进行攻击的。

A.1

B.2

C.3

D.4

正确答案：C

8.[单选题]域名服务系统(DNS)的功能是( )

A.完成域名和IP地址之间的转换

B.完成域名和网卡地址之间的转换

C.完成主机名和IP地址之间的转换

D.完成域名和电子邮件地址之间的转换

正确答案：A

9.[单选题]从风险管理的角度，以下哪种方法不可取?( )

A.接受风险

B.分散风险

C.转移风险

D.拖延风险

正确答案：D

10.[单选题]Windows主机推荐使用( )格式。

A.NTFS

B.FAT32

C.FAT

D.Linux

正确答案：A

11.[单选题]通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的IP包时会出现崩溃，请问这种攻击属于何种攻击?( )

A.拒绝服务(DoS)攻击

B.扫描窥探攻击

C.系统漏洞攻击

D.畸形报文攻击

正确答案：D

12.[单选题]应用网关防火墙在物理形式上表现为?( )

A.网关

B.堡垒主机

C.路由

D.交换机

正确答案：B

13.[单选题]在入侵检测的基础上，锁定涉嫌非法使用的用户，并限制和禁止该用户的使用。这种访问安全控制是?( )

A.入网访问控制

B.权限控制

C.网络检测控制

D.防火墙控制

正确答案：C

14.[单选题]防火墙截取内网主机与外网通信，由防火墙本身完成与外网主机通信，然后把结果传回给内网主机，这种技术称为( )。

A.内容过滤

B.地址转换

C.透明代理

D.内容中转

正确答案：C

15.[单选题]监听的可能性比较低的是( )数据链路。

A.Ethernet

B.电话线

C.有线电视频道

D.无线电

正确答案：B

16.[单选题]我国的国家秘密分为几级?( )

A.3

B.4

C.5

D.6

正确答案：A

17.[单选题]使网络服务器中充斥着大量要求回复的信息，消息带宽，导致网络或系统停止正常服务，这属于什么攻击类型?( )

A.拒绝服务

B.文件共享

C.BIND漏洞

D.远程过程调用

正确答案：A

18.[单选题]包过滤防火墙工作的好坏关键在于?( )

A.防火墙的质量

B.防火墙的功能

C.防火墙的过滤规则设计

D.防火墙的日志

正确答案：C

19.[单选题]关于WEB应用软件系统安全，说法正确的是( )

A.Web应用软件的安全性仅仅与WEB应用软件本身的开发有关

B.系统的安全漏洞属于系统的缺陷，但安全漏洞的检测不属于测试的范畴

C.黑客的攻击主要是利用黑客本身发现的新漏洞

D.以任何违反安全规定的方式使用系统都属于入侵

正确答案：D

20.[单选题]RSA使用不方便的最大问题是( )。

A.产生密钥需要强大的计算能力

B.算法中需要大数

C.算法中需要素数

D.被攻击过很多次

正确答案：A

21.[单选题]关于CA和数字证书的关系，以下说法不正确的是( )。

A.数字证书是保证双方之间的通讯安全的电子信任关系，它由CA签发

B.数字证书一般依靠CA中心的对称密钥机制来实现

C.在电子交易中，数字证书可以用于表明参与方的身份

D.数字证书能以一种不能被假冒的方式证明证书持有人身份

正确答案：B

22.[单选题]在以下隧道协议中，属于三层隧道协议的是( )。

A.L2F

B.PPTP

C.L2TP

D.IPSec

正确答案：D

23.[单选题]在大多数情况下，病毒侵入计算机系统以后，( )。

A.病毒程序将立即破坏整个计算机软件系统

B.计算机系统将立即不能执行我们的各项任务

C.病毒程序将迅速损坏计算机的键盘、鼠标等操作部件

D.一般并不立即发作，等到满足某种条件的 时候，才会出来活动捣乱、破坏

正确答案：D

简答题

1. TCP/IP的4层协议与OSI参考模型的7层协议是如何对应的?

|  |  |  |
| --- | --- | --- |
| **OSI 7 层网络模型** | **TCP/IP 4 层模型** | **对应网络协议** |
| 应用层 | 应用层 | Telnet、Rlogin、SNMP、Gopher、SMTP、DNS |
| 表示层 |
| 会话层 |
| 传输层 | 传输层 | TCP、UDP |
| 网络层 | 网络层 | IP、ICMP、ARP、RARP、AKP、UUCP |
| 数据链路层 | 网络接口层 | FDDI、Ethernet、Arpanet、PDN、SLIP |
| 物理层 | IEEE 802.1A、IEEE 802.2 - IEEE 802.11 |

1. VPN 技术有哪些主要特点?

VPN具有存以下技术特点:

**1)安全性高。**VPN 使用通信协议、身份验证和数据加密等技术保证其网络通信传输的安全性。客户机先向VPN服务器发出请求，服务器响应请求并要求客户机输入身份认证信息，之后客户机发送认证信息，服务器通过数据库检查认证该用户的远程访问权限，对通过认证的用户服务器会进行接收并连接，身份验证过程中所使用的公有密钥都需要加密。

**2)费用低、应用广。**远程用户或机构都可以利用VPN通过Internet访问网络，这比传统网络访问方式的费用少很多，可节省购买、管理和维护通信设备的费用且应用广泛。

**3)管理便利。**构建VPN只需很少的专用的网络设备及线路，且网络管理非常简便。对于远程访问的企事业机构或用户，只需要通过公用网络端口或Interet即可进入机构网络，网络管理如同使用微信群，其主要工作由公用网负责。

**4)灵活性强。**VPN支持通过各种网络的任何类型的数据流，支持多种类型的传输媒介，并可以同时传输图像、语音和其他数据等需求。

**5)服务质量好。**可满足机构不同等级的服务质量(QoS)需求。不同用户和业务对QoS要求差别较大，如对于移动用户，提供广泛连接和覆盖性是保证VPN服务的一个主要因素;对于拥有众多分支机构的专线VPN，交互式内网应用要求网络具有良好的稳定性:

1. 信息安全保障体系架构具体包括哪5个部分?
2. **‌信息安全战略**‌：为信息安全提供总体方向和指引。
3. **‌信息安全政策和标准**‌：制定并规范信息安全的相关政策和标准。
4. **‌信息安全运作**‌：确保信息安全策略在日常运营中的有效实施。
5. **‌信息安全管理**‌：对信息安全进行计划、组织、指导和控制。
6. **‌信息安全技术**‌：采用技术手段保障信息的安全性和完整性‌。‌
7. 如何理解“七分管理，三分技术，运作贯穿始终”?
8. ‌**管理为核心**‌：管理在信息安全中占据主导地位，通过制度、规范进行约束和控制，确保各项安全措施得到有效执行。管理涉及计划、组织、协调、控制和决策，是信息安全工作的关键。
9. ‌**技术为支撑**‌：技术是实现信息安全的重要手段，但仅凭技术难以确保全面的安全。技术需要与管理相结合，为信息安全提供有力保障。
10. ‌**运作是关键**‌：信息安全运作是管理和技术在日常工作中的具体执行，是信息安全工作的核心。通过运作，将管理和技术紧密结合，形成有效的安全防护体系。
11. 防火墙、IDS与IPS的区别。

入侵检测系统(DDS)的主要功能是通过对网络信息的检测分析，掌握网络系统的安全状况，便于指导网络系统安全保护、安全策略的确立和调整。入侵防御系统(IPS)的主要功能是通过对网络安全策略进行检测分析并阻断黑客攻击。DS需要部署在网络内部，监控范围可以覆盖整个子网，包括来自外部的数据和内部终端之间传输的数据。IPS 则需要部署在网络边界，主要侧重检测防御来自外部网络的入侵攻击行为。防火墙是通过访问控制策略，检测流经的网络流量等异常行为，拦截违反安全策略的数据包并告警。IDS通过监视网络或系统资源，检测违反安全策略的行为或攻击事件并发出报警。传统的防火墙旨在拒绝明显可疑的网络流量，但仍然允许某些流量通过，因此防火墙对于很多入侵攻击无计可施。绝大多数IDS都是被动的，在发生攻击之前，往往无法预测警报。而IPS可侧重提供主动防护，其设计思路是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才告警。IPS通过一个网络端口接收来自外部系统的流量，经过检测、分析并确认其中无异常活动或可疑内容后，再通过另外一个端口将其传送到内部系统，因此，有问题的数据包以及所有来自同一数据流的后续数据包，都能在IPS设备中被阻断或清除。

1. 什么是异常检测?什么是特征检测?

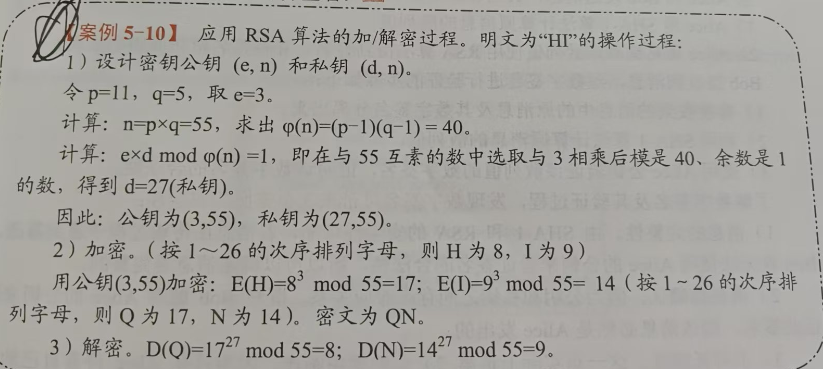
**1·‌异常检测‌：**

‌**定义**‌：异常检测是一种基于行为或正常活动模式的分析技术，其主要目标是识别出与预期正常行为模式显著不同的活动或事件。

**2·特征检测**‌：

‌**定义**‌：特征检测是一种基于已知威胁或攻击特征的分析技术，它通过匹配已知的特征模式来识别潜在的威胁或攻击。

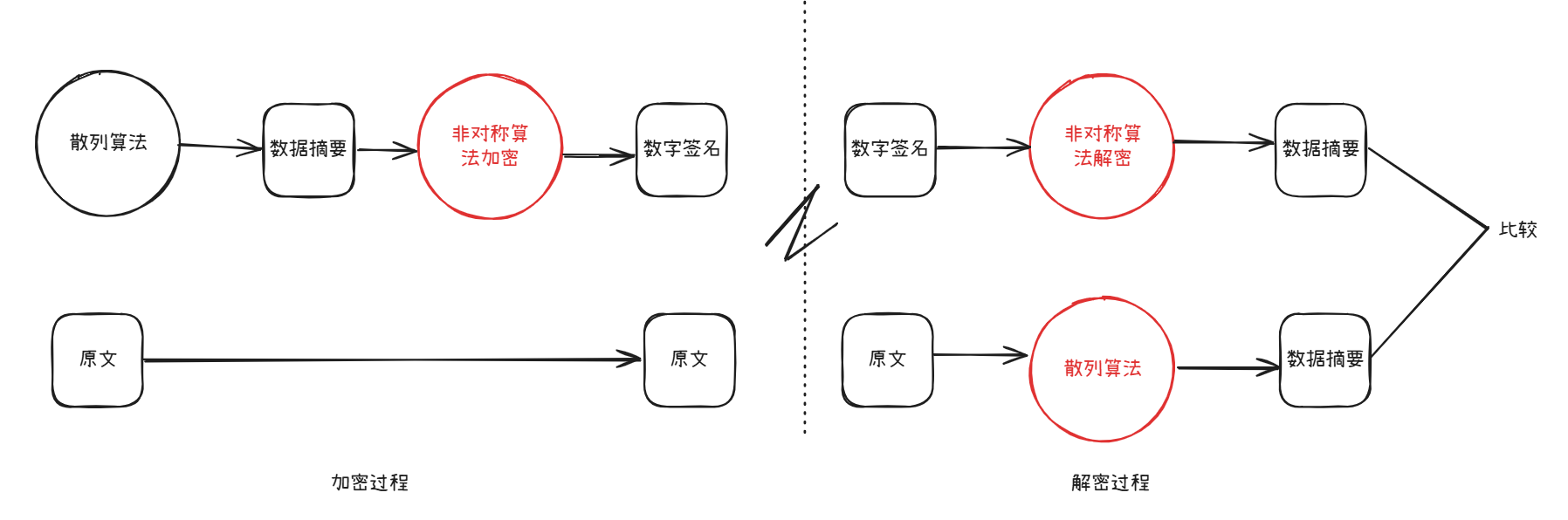
1. P117



1. 已知 RSA 算法中，素数p=5，q=7，模数n=35，公开密钥e=5，密文 c=10，求明文，试用手工完成 RSA 公开密钥密码体制算法加密运算。**（参7）**
2. 简述数字签名技术的实现过程。P132

对一个电子文件进行数字签名并在网上传输，通常需要实现的过程包括:网上身份认证、进行签名和对签名的验证。

网上通信的双方，在互相认证身份之后，即可发送签名的数据电文。数字签名的全过程分为两大部分，即签名与验证。数字签名与验证的过程和技术实现的原理



1. 简述计算机病毒的特点有哪些。P157
2. ‌**隐蔽性**‌：病毒隐藏于合法程序或数据中，用户不易察觉‌。
3. ‌**传染性**‌：病毒能自我复制，迅速从已感染计算机扩散至未感染计算机‌。
4. ‌**潜伏性**‌：病毒有潜伏期，特定条件下才激活‌。
5. ‌**破坏性**‌：病毒会占用资源、降低效率、破坏系统或数据‌。
6. ‌**可触发性**‌：病毒有触发条件，满足时即激活传染或破坏机制‌。
7. ‌**寄生性**‌：病毒需寄生在合法程序中，以该程序为生存环境‌。
8. ‌**非授权可执行性**‌：病毒在用户不知情的情况下窃取系统控制。
9. 计算机中毒的异常表现有哪些?AI（例5种表现）P160
10. ‌**系统运行缓慢**‌：病毒可能会占用大量的系统资源，如CPU、内存等，导致计算机运行速度明显变慢，程序打开、文件处理等操作变得迟缓。
11. ‌**频繁死机或重启**‌：病毒可能会破坏系统文件或干扰正常的系统运行，导致计算机频繁出现死机、蓝屏或自动重启的情况。
12. ‌**文件或数据丢失、损坏**‌：病毒可能会删除、修改或加密用户的重要文件和数据，导致数据丢失或无法访问。有时，即使文件看似存在，但内容可能已经被破坏或篡改。
13. ‌**网络异常**‌：病毒可能会修改网络设置，导致网络连接不稳定或无法连接网络。有些病毒还会利用网络资源进行传播，导致网络流量异常增加。
14. ‌**弹出不明窗口或广告**‌：病毒可能会在用户计算机上安装恶意软件或广告插件，导致在使用计算机时频繁弹出不明窗口、广告或警告信息，影响用户正常使用体验。
15. 如何清除计算机病毒?AI P166
16. ‌**杀毒软件清除**‌：使用杀毒软件进行全面扫描，确保病毒库最新，选择全面扫描并立即执行‌。
17. ‌**主引导区恢复**‌：若感染引导型病毒，采用备份的主引导扇区文件覆盖恢复‌。
18. ‌**程序覆盖法**‌：针对文件型病毒，重新安装被感染程序，覆盖所有文件‌。
19. ‌**格式化磁盘**‌：对于顽固病毒，采用格式化或低级格式化磁盘彻底清除‌。
20. ‌**手工清除**‌：适用于所有病毒，特别是新出现或未知病毒，需专业人员操作‌。
21. ‌**专用工具清理**‌：使用如AdwCleaner等工具，扫描并删除广告软件和潜在威胁‌。
22. ‌**清理启动项和进程**‌：通过任务管理器和启动项管理，结束并禁用可疑进程和启动项‌。
23. SYN Flood 攻击的原理是什么? P192

SYN Flood攻击是一种拒绝服务（DoS）攻击，其原理在于利用TCP协议的三次握手过程。攻击者向目标服务器发送大量伪造的TCP连接请求（SYN数据包），服务器在接收到这些请求后会回复SYN-ACK包，并等待客户端的ACK确认以建立连接。然而，攻击者并不发送ACK确认，导致服务器维持大量的半连接状态，即SYNC\_RECV状态。由于服务器的资源（如内存、CPU等）有限，这些半连接会消耗大量资源，最终使得服务器无法响应合法的连接请求，从而实现拒绝服务攻击‌。

简而言之，SYN Flood攻击通过伪造大量的TCP连接请求，使服务器资源耗尽，无法为正常用户提供服务。

1. 防火墙如何阻止 SYN Flood攻击?（2种模式） p192

**‌SYN网关模式‌：**

‌**原理‌**：防火墙在收到服务器的SYN/ACK包后，会立即代替客户端发送一个ACK包给服务器，使服务器快速进入连接状态。

‌**效果‌**：减少了服务器的半连接数，有效抵御SYN Flood攻击。

‌**被动SYN网关模式‌：**

‌**设置‌**：防火墙设置较短的SYN请求超时参数。

‌**原理**‌：若客户端在防火墙计时器到期前未发送ACK包，防火墙会向服务器发送RST包，删除半连接。

‌**效果‌**：由于防火墙的超时参数远小于服务器，因此能更早地释放资源，防止攻击。