网络与信息安全技术期末考试题库及答案全集文档

(可以直接使用，可编辑 实用优质文档，欢迎下载)

网络与信息安全技术 A 卷

一、　单项选择题（每小题 2 分，共 20 分）

1．信息安全的基本属性是_____。

A. 保密性B.完整性

C. 可用性、可控性、可靠性 **D. A，B，C 都是**

2．假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于_____。

A. 对称加密技术B. 分组密码技术

C. 公钥加密技术D. 单向函数密码技术

3．密码学的目的是_____。

A. 研究数据加密B. 研究数据解密

C. 研究数据保密D. 研究信息安全

4．A 方有一对密钥（$K_{A\,公开}$，$K_{A\,秘密}$），B 方有一对密钥（$K_{B\,公开}$，$K_{B\,秘密}$），A 方向 B 方发送数字签名 M，对信息 M 加密为：M'= $K_{B\,公开}$（$K_{A\,秘密}$（M））。B 方收到密文的解密方案是_____。

A. $K_{B\,公开}$（$K_{A\,秘密}$（M'））　　B. $K_{A\,公开}$（$K_{A\,公开}$（M'））

C. $K_{A\,公开}$（$K_{B\,秘密}$（M'））　　D. $K_{B\,秘密}$（$K_{A\,秘密}$（M'））

5．数字签名要预先使用单向Hash函数进行处理的原因是_____。

A. 多一道加密工序使密文更难破译

B. 提高密文的计算速度

C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

D. 保证密文能正确还原成明文

6．身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是____。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

7．防火墙用于将 Internet 和内部网络隔离_____。

A. 是防止 Internet 火灾的硬件设施

B.是网络安全和信息安全的软件和硬件设施

C.是保护线路不受破坏的软件和硬件设施

D.是起抗电磁干扰作用的硬件设施

8．PKI支持的服务不包括_____。

A. 非对称密钥技术及证书管理B. 目录服务

C. 对称密钥的产生和分发**D.** 访问控制服务

9．设哈希函数 H 有 128 个可能的输出(即输出长度为 128 位)，如果 H 的 k 个随机输入中至少有两个产生相同输出的概率大于 0.5，则 k 约等于____。

A．2^{128}B．2^{64}

C．2^{32}　　D．2^{256}

10．Bell-LaPadula 模型的出发点是维护系统的_____，而 Biba 模型与 Bell-LaPadula 模型完全对立，它修正了 Bell-LaPadula 模型所忽略的信

息的_____问题。它们存在共同的缺点：直接绑定主体与客体，授权工作困难。

A. 保密性　可用性　　B. 可用性　保密性

C. 保密性　完整性　　D. 完整性　保密性

二、　填空题（每空 2 分，共 40 分）

1. ISO 7498-2 确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和不可否认。同时，ISO 7498-2 也确定了八类安全机制，即加密机制、数据签名机制、访问控制机制、数据完整性机制、认证交换、业务填充机制、路由控制机制和公证机制。
2. 古典密码包括代替密码和置换密码两种，对称密码体制和非对称密码体制都属于现代密码体制。传统的密码系统主要存在两个缺点：一是密钥管理与分配问题；二是认证问题。在实际应用中，对称密码算法与非对称密码算法总是结合起来的，对称密码算法用于加密，而非对称算法用于保护对称算法的密钥。
3. 根据使用密码体制的不同可将数字签名分为基于对称密码体制的数字签名和基于公钥密码体制的数字签名，根据其实现目的的不同，一般又可将其分为直接数字签名和可仲裁数字签名。
4. DES 算法密钥是 64 位，其中密钥有效位是 56 位。RSA 算法的安全是基于分解两个大素数的积的困难。
5. 密钥管理的主要内容包括密钥的生成、分配、使用、存储、备份、恢复和销毁。密钥生成形式有两种：一种是由中心集中生成，另一种是由个人分散生成。
6. 认证技术包括站点认证、报文认证和身份认证，而身份认证的方法主要有口令、磁卡和智能卡、生理特征识别、零知识证明。
7. NAT 的实现方式有三种，分别是静态转换、动态转换、端口多路复用。
8. 数字签名是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

三、　简答题（每小题 8 分，共 24 分）

1、网络信息安全的含义？

答：网络信息安全是指利用网络管理控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可使用性受到保护。计算机网络安全包括两个方面，即物理安全和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安安全包括信息的完整性、保密性和可用性。

2、什么是入侵检测系统？

答：入侵检测系统（简称“IDS”）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处便在于，IDS 是一种积极主动的安全防护技术。 IDS 最早出现在 1980 年 4 月。 1980 年代中期，IDS 逐渐发展成为入侵检测专家系统（IDES）。

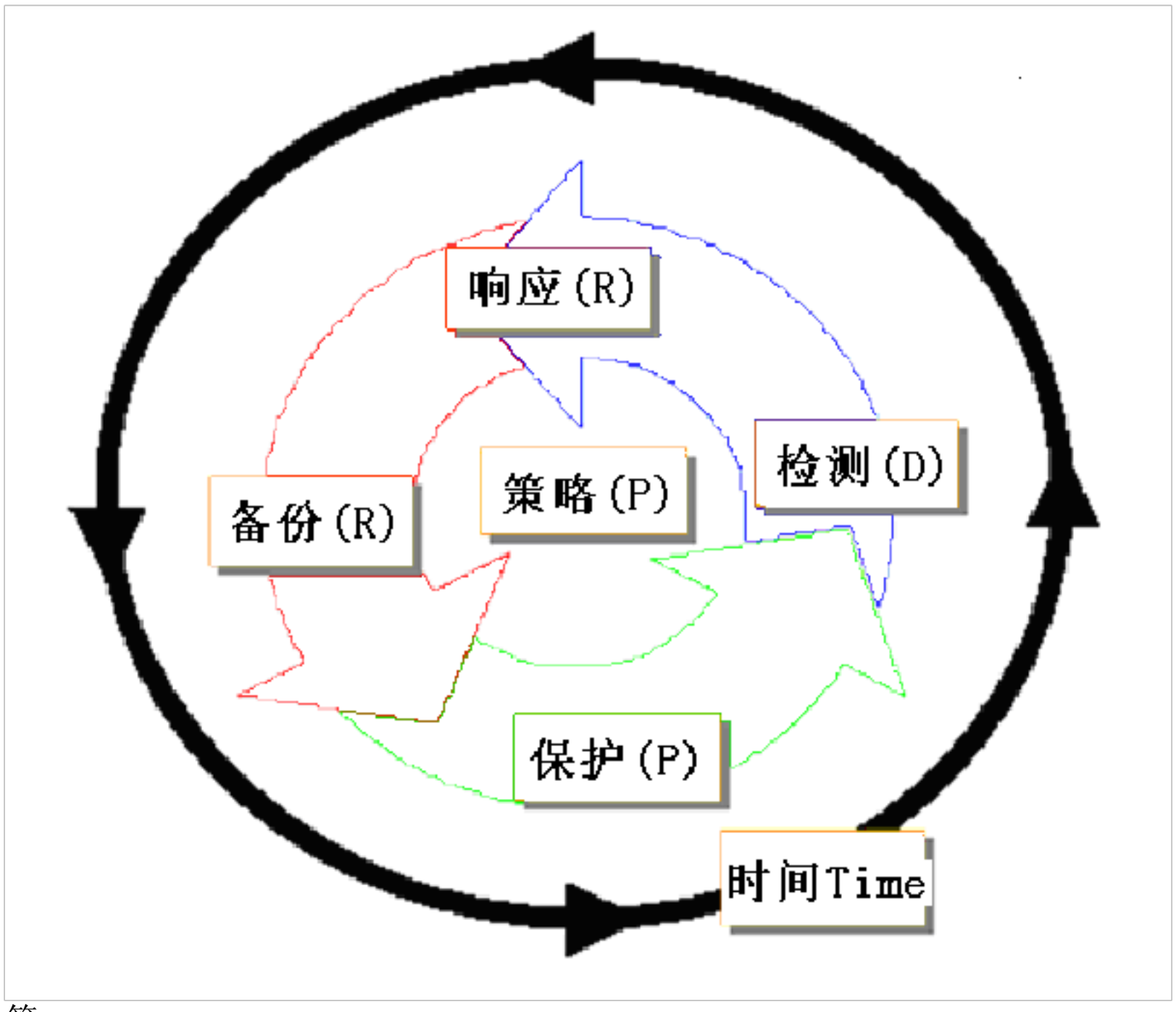
3、请说明 DES 算法的基本过程？

答：DES 加密算法特点：分组比较短、密钥太短、密码生命周期短、运算速度较慢。

DES 工作的基本原理是，其入口参数有三个:key、data、mode。 key 为加密解密使用的密钥，data 为加密解密的数据，mode 为其工作模式。当模式为加密模式时，明文按照 64 位进行分组，形成明文组，key 用于对数据加密，当模式为解密模式时，key 用于对数据解密。实际运用中，密钥只用到了 64 位中的 56 位，这样才具有高的安全性。

四、　分析题（16 分）

1．下图表示的是 P2DR2 动态安全模型，请从信息安全安全角度分析此模型？



答：

P2DR2 动态安全模型研究的是基于企业网对象、依时间及策略特征的（Policy Protection Detection Response Restore）动态安全模型结构，由策略、防护、检测、响应和恢复等要素构成，是一种基于闭环控制、主动防御的动态安全模型。通过区域网络的路由及安全策略分析与制定，在网络内部及边界建立实时检测、监测和审计机制，采取实时、快速动态响应安全手段，应用多样性系统灾难备份恢复、关键系统冗余设计等方法，构造多层次、全方位和立体的区域网络安全环境。

安全策略不仅制定了实体元素的安全等级，而且规定了各类安全服务互动的机制。每个信任域或实体元素根据安全策略分别实现身份验证、访问控制、安全通信、安全分析、安全恢复和响应的机制选择。

网络与信息安全技术 B 卷

一、　单项选择题（每小题 2 分，共 20 分）

1、关于密码学的讨论中，下列（D）观点是不正确的。

A、密码学是研究与信息安全相关的方面如机密性、完整性、实体鉴别、抗否认等的综合技术

B、密码学的两大分支是密码编码学和密码分析学

C、密码并不是提供安全的单一的手段，而是一组技术

D、密码学中存在一次一密的密码体制，它是绝对安全的

2、在以下古典密码体制中，属于置换密码的是（B）。

A、移位密码 B、倒序密码

C、仿射密码 D、PlayFair 密码

3、一个完整的密码体制，不包括以下（ C ）要素。

A、明文空间 B、密文空间

C、数字签名 D、密钥空间

4、关于 DES 算法，除了（C）以外，下列描述 DES 算法子密钥产生过程是正确的。

A、首先将 DES 算法所接受的输入密钥 K（64 位），去除奇偶校验位，得到 56 位密钥（即经过 PC-1 置换，得到 56 位密钥）

B、在计算第 i 轮迭代所需的子密钥时，首先进行循环左移，循环左移的位数取决于 i 的值，这些经过循环移位的值作为下一次循环左移的输入

C、在计算第 i 轮迭代所需的子密钥时，首先进行循环左移，每轮循环左移的位数都相同，这些经过循环移位的值作为下一次循环左移的输入

D、然后将每轮循环移位后的值经 PC-2 置换，所得到的置换结果即为第 i 轮所需的子密钥 Ki

5、2000 年 10 月 2 日，NIST 正式宣布将（B）候选算法作为高级数据加密标准，该算法是由两位比利时密码学者提出的。

A、MARS　　B、Rijndael

C、Twofish　　D、Bluefish

6、根据所依据的数学难题，除了（A）以外，公钥密码体制可以分为以下几类。

A、模幂运算问题　　B、大整数因子分解问题

C、离散对数问题　　D、椭圆曲线离散对数问题

7、密码学中的杂凑函数（Hash 函数）按照是否使用密钥分为两大类：带密钥的杂凑函数和不带密钥的杂凑函数，下面（C）是带密钥的杂凑函数。

A、MD4　　B、SHA-1

C、whirlpool　　D、MD5

8、完整的数字签名过程（包括从发送方发送消息到接收方安全的接收到消息）包括（C ）和验证过程。

A、加密　　B、解密

C、签名　　D、保密传输

9、除了（D）以外，下列都属于公钥的分配方法。

A、公用目录表　　B、公钥管理机构

C、公钥证书　　D、秘密传输

10、密码学在信息安全中的应用是多样的，以下（ A ）不属于密码学的具体应用。

A、生成种种网络协议　　B、消息认证，确保信息完整性

C、加密技术，保护传输信息　　D、进行身份认证

二、填空题（每空 2 分，共 40 分）

1、信息安全中所面临的威胁攻击是多种多样的，一般将这些攻击分为两大类（主动攻击）和被动攻击。其中被动攻击又分为（消息内容的泄露）和（进行业务流分析）。

2、密码技术的分类有很多种，根据加密和解密所使用的密钥是否相同，可以将加密算法分为：对称密码体制和（非对称密码体制），其中对称密码体制又可分为两类，按字符逐位加密的（序列密码）和按固定数据块大小加密的（分组密码）。

3、密码分析是研究密码体制的破译问题，根据密码分析者所获得的数据资源，可以将密码分析（攻击）分为：（惟密文分析）、已知明文分析（攻击）、（选择明文分析）和选择密文分析（攻击）。

4、古典密码学体制对现代密码学的研究和学习具有十分重要的意义，实现古典密码体制的两种基本方法（代换）和（置换）仍是构造现代对称分组密码的核心方式。

5、（DES）是美国国家标准局公布的第一个数据加密标准，它的分组长度为（64）位，密钥长度为（64（56））位。

6、1976 年，美国两位密码学者 Diffe 和 Hellman 在该年度的美国计算机会议上提交了一篇论文，提出了（公钥密码体制）的新思想，它为解决传统密码中的诸多难题提出了一种新思路。

7、Elgamal 算法的安全性是基于（离散对数问题），它的最大特点就是在加密过程中引入了一个随机数，使得加密结果具有（不确定性），并且它的密文长度是明文长度的（两）倍。该算法的变体常用来进行数据签名。

8、密码系统的安全性取决于用户对于密钥的保护，实际应用中的密钥种类有很多，从密钥管理的角度可以分（初始密钥）、（会话密钥）、密钥加密密钥和（主密钥）。

三、简答题（每小题 12 分，共 24 分）

1、信息安全有哪些常见的威胁？信息安全的实现有哪些主要技术措施？

答：常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击，恶意代码。信息安全的实现可以通过物理安全技术，系统安全技术，网络安全技术，应用安全技术，数据加密技术，认证授权技术，访问控制技术，审计跟踪技术，防病毒技术，灾难恢复和备份技术。

2、什么是密码分析，其攻击类型有哪些？ DES 算法中 S 盒的作用是什么？

答：密码分析是指研究在不知道密钥的情况下来恢复明文的科学。攻击类型有只有密文的攻击，已知明文的攻击，选择明文的攻击，适应性选择明文攻击，选择密文的攻击，选择密钥的攻击，橡皮管密码攻击。 S 盒是 DES 算法的核心。其功能是把 6bit 数据变为 4bit 数据。

四、　　分析题（16 分）

试说明黑客攻击的一般流程及其技术和方法

答：

期末考试复习

1、考试形式：闭卷

2、考试时间：**2** 小时

3、试卷题型及分数分配：**6** 种题型，共 **100** 分。

（**1**）单项选择题：**1** 分**/**题 **X20** 题**=20** 分；

（**2**）填空题：**1** 分**/**空 **X10** 空**=10** 分；

（**3**）判断题：**1** 分**/**题 **X10** 题**=10** 分；

（**4**）名词解释：**5** 分**/**题 **X4** 题**=20** 分；

（**5**）简答题：**8** 分**/**题 **X3** 题**=24** 分；

（**6**）论述题：**16** 分**/**题 **X1** 题**=16** 分。

4、考试范围

第一章：网络技术基础

（**1**）计算机网络的分类

计算机网络可分为局域网、广域网和城域网。

●局域网：局域网(Local Area Network，简称 LAN)是将较小地理区域内的计算机或数据终端设备连接在一起的通信网络。局域网覆盖的地理范围比较小，它常用于组建一个企业、校园、楼宇和办公室内的计算机网络。

● 广域网：广域网(Wide Area Network， 简称 WAN)是在一个广阔的地理区域内进行数据、语音、图像等信息传输的通信网络。广域网覆盖的地理区域较大，它可以覆盖一个城市、一个国家、一个洲乃至整个地球。

广域网覆盖的范围比局域网（LAN）和城域网（MAN）都广。广域网的通信子网主要使用分组交换技术。广域网的通信子网可以利用公用分组交换网、卫星通信网和无线分组交换网，它将分布在不同地区的局域网或计算机系统互连起来，达到资源共享的目的。如互联网是世界范围内最大的广域网。

城域网：城域网(Metropolitan Area Network， 简称 MAN)是介于局域网和广域网之间的一种高速网络，它的覆盖范围在一个城市内。属宽带局域网。由于采用具有有源交换元件的局域网技术，网中传输时延较小，它的传输媒介主要采用光缆，传输速率在 100 兆比特/秒以上。

（**2**）**DNS** 服务器的概念

DNS 服务器是计算机域名系统 (Domain Name System 或 Domain Name Service) 的缩写，它是由解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应 IP 地址，并具有将域名转换为 IP 地址功能的服务器。其中域名必须对应一个 IP 地址，而 IP 地址不一定有域名。域名系统采用类似目录树的等级结构。域名服务器为客户机/服务器模式中的服务器方，它主要有两种形式：主服务器和转发服务器。将域名映射为 IP 地址的过程就称为“域名解析”。

（**3**）**TCP/IP** 协议的概念及各层的功能。

TCP/IP 协议

TCP/IP 是 Transmission Control Protocol/Internet Protocol（传输控制协议/互联网协议）的缩写。美国国防部高级研究计划局 DARPA 为了实现异种网络之间的互连与互通， 大力资助互联网技术的开发，于 1977 年到 1979 年间推出目前形式的 TCP/IP 体系结构和协议。在 1980 年左右，ARPA 开始将 ARPANET 上的所有机器转向 TCP/IP 协议，并以 ARPANET 为主干建立了 Internet。

TCP/IP 也是一个分层的网络协议，不过它与 OSI 模型所分的层次有所不同。TCP/IP 从底至顶分为网络接口层、网络层、传输层、应用层等 4 个层次。

●网络接口层：这是 TCP/IP 协议的最低一层，包括有多种逻辑链路控制和媒体访问协议。

网络接口层的功能是接收 IP 数据报并通过特定的网络进行传输，或从网络上接收物理帧，抽取出 IP 数据报并转交给网际层。

●网络层（IP 层）：该层包括以下协议：IP（ /Internet Protocol，网际协议）、ICMP（Internet Control Message Protocol，因特网控制报文协议）、ARP（Address Resolution Protocol，地址解析协议）、RARP（Reverse Address Resolution Protocol，反向地址解析协议）。该层负责相同或不同网络中计算机之间的通信，主要处理数据报和路由。在 IP 层中，ARP 协议用于将 IP 地址转换成物理地址，RARP 协议用于将物理地址转换成 IP 地址，ICMP 协议用于报告差错和传送控制信息。IP 协议在 TCP/IP 协议组中处于核心地位。

●传输层：该层提供 TCP（传输控制协议）和 UDP（User Datagram Protocol，用户数据报协议）两个协议，它们都建立在 IP 协议(网络协议) 的基础上，其中 TCP 提供可靠的面向连接服务，UDP 提供简单的无连接服务。传输层提供端到端，即应用程序之间的通信，主要功能是数据格式化、数据确认和丢失重传等。

●应用层：TCP/IP 协议的应用层相当于 OSI 模型的会话层、表示层和应用层，它向用户提供一组常用的应用层协议，其中包括：Telnet（远程登录）、SMTP（简单邮件传输协议）、DNS（域名系统）等。此外，在应用层中还包含有用户应用程序，它们均是建立在 TCP/IP 协议组之上的专用程序。

第二章：网络安全概述

（**1**）网络安全的定义，会从用户和运营商（管理者）的角度解释什么是网络安全。

网络安全从其本质来讲就是网络上的信息安全。他涉及的领域相当广泛。这是因为目前的公用通信网络中存在着各种各样的安全漏洞和威胁。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性和可控性的相关技术和理论，都是网络安全的研究领域。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

从用户的角度来说，他们希望涉及到个人隐私和商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对用户的利益和隐私造成损害和侵犯。同时他们希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

从网络运营商和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源的非法占用和非法控制等威胁，制止和防御网络“黑客”的攻击。

因此，人们在不同的网络环境和网络应用中对网络安全的理解是不同的。

（**2**）网络安全有哪些安全属性，各个安全属性是如何定义的。

网络安全的属性

●机密性：机密性是指保证信息与信息系统不被非授权者所获取与使用，主要防范措施是密码技术。

在网络系统的各个层次上有不同的机密性及相应的防范措施。在物理层，要保证系统实体不以电磁的方式(电磁辐射、电磁泄漏)向外泄漏信息，主要的防范措施是电磁屏蔽技术、加密干扰技术等。在运行层面，要保障系统依据授权提供服务，使系统任何时候不被非授权人所使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取漏洞扫描、隔离、防火墙、访问控制、入侵检测、审计取证等防范措施。这类属性有时也称为可控性。

在数据处理、传输层面，要保证数据在传输、存储过程中不被非法获取、解析，主要防范措施是数据加密技术。

●完整性：完整性是指信息是真实可信的，其发布者不被冒充，来源不被伪造，内容不被篡

改，主要防范措施是校验与认证技术。
在运行层面，要保证数据在传输、存储等过程中不被非法修改，防范措施是对数据的截获、篡改与再送采取完整性标识的生成与检验技术。要保证数据的发送源头不被伪造，对冒充信息发布者的身份、虚假信息发布来源采取身份认证技术、路由认证技术，这类属性也可称为真实性。
●可用性：可用性是指保证信息与信息系统可被授权人正常使用，主要防范措施是确保信息与信息系统处于一个可靠的运行状态之下。
在物理层，要保证信息系统在恶劣的工作环境下能正常运行，主要防范措施是对电磁炸弹、信号插入采取抗干扰技术、加固技术等。在运行层面，要保证系统时刻能为授权人提供服务，对网络被阻塞、系统资源超负荷消耗、病毒、黑客等导致系统崩溃或死机等情况采取过载保护、防范拒绝服务攻击、生存技术等防范措施。
保证系统的可用性，使得发布者无法否认所发布的信息内容，接收者无法否认所接收的信息内容，对数据抵赖采取数字签名防范措施，这类属性也称为抗否认性。
从上面的分析可以看出，维护信息载体的安全与维护信息自身的安全两个方面都含有机密性、完整性、可用性这些重要属性。

（**3**）**GB17859** 把计算机信息系统的安全保护能力划分的 **5** 个等级。
我国的 GB17859 中，去掉了这两个级别，对其他 5 个级别也赋予了新意。C1、C2、B1、B2、B3

4、考试范围
第三章：主机网络安全及访问控制安全
（**1**）主机网络安全的概念。
计算机安全分为两部分，一个是主机安全，一个是网络安全。主机安全主要是考虑保护合法用户对于授权资源的使用，防止非法入侵者对于系统资源的侵占与破坏。其最常用的办法是利用操作系统的功能，如 Unix 的用户认证、文件访问权限控制、帐号审计等。网络安全主要考虑的是网络上主机之间的访问控制，防止来自外部网络的入侵，保护数据在网上传输时不被泄密和修改。其最常用的方法是防火墙、加密等。
主机网络安全技术是一种主动防御的安全技术，它结合网络访问的网络特性和操作系统特性来设置安全策略，可以根据网络访问的访问者及访问发生的时间、地点和行为来决定是否允许访问继续进行，实现对于同一用户在不同的场所拥有不同的权限，从而保证合法用户的权限不被非法侵占。

（**2**）访问控制的两种类型。（系统、网络）
入侵检测系统通常分为基于主机和基于网络两类。
基于主机入侵检测的主要特征是使用主机传感器监控本系统的信息。这种技术可以用于分布式、加密、交换的环境中监控，把特定的问题同特定的用户联系起来。它能够实时监视可疑的连接，检查系统日志，监视非法访问和典型应用。它还可针对不同操作系统的特点判断应用层的入侵事件，对系统属性、文件属性、敏感数据、攻击进程结果进行监控。它能够精确地判断入侵事件，并对入侵事件迅速做出反应，结合主机上的包过滤功能模块切断来自可疑地址的网络连接。
基于网络的入侵检测主要特征是网络监控传感器监控包监听器收集的信息。它使用原始的网络包作为数据源，它将网络数据中检测主机的网卡设为混杂模式，该主机实时接收和分析网络中流动的数据包，从而检测是否存在入侵行为，但它不能审查加密数据流的内容，对高速

网络不是特别有效。

（**3**）掌握基于角色的访问控制模型，会画出 **RBAC96** 模型图。

基于角色的访问控制(Role- Based Access Control,RBAC)的基本思想就是根据安全策略划分出不同的角色,资源访问许可被封装在角色中，用户被指派到角色，用户通过角色间接地访问资源。

b. RBAC 的最大优点在于它能够灵活表达和实现组织的安全政策,使管理员从访问控制底层的具体实现机制中脱离出来,十分接近日常的组织管理规则。RBAC 被认为是一种更普遍适用的访问控制模型,可以有效地表达和巩固特定事务的安全策略,有效缓解传统安全管理处理瓶颈问题。

c.角色与组的差别:

●角色既是用户的集合，又是操作许可的集合；组通常是作为用户的集合,而不是操作许可的集合。

●角色是表达组织安全策略的部件，属于安全策略，抽象级高；组是机制，是实现工具,抽象级低。两者是策略与实现机理的关系。

RBAC96 模型

第四章：密码技术

（**1**）比较对称式密码体制和非对称密码体制。

对称密码技术就是加密密钥和解密密钥相同的这类密码体制，它采用的解密算法是加密算法的逆运算。该体制的特点是在保密通信系统发送者和接收者之间的密钥必须安全传送，而双方通信所用的秘密密钥必须妥善保管。

对称密码技术的安全性依赖于以下两个因素：第一，加密算法必须是足够强的，仅仅基于密

文本身去解密信息在实践上是不可能的；第二，加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性。因此，没有必要确保算法的秘密性，而需要的是保证密钥的秘密性。
目前计算机网络主要采用两种密码体制:对称密钥体制和非对称密钥体制。对称密钥体制的加密密钥和解密密钥是相同的,只要知道加密密钥就能推算出解密密钥,通信双方分别持有加密密钥和解密密钥。在使用对称密码技术进行秘密通信时，任意两个不同用户之间都应该使用互不相同的密钥。如果一个网络中有 n 个用户，他们之间可能会进行秘密通信，这时网络中共需 n(n—1)/2 个密钥(其中每个用户都需要保存 n—1 个密钥)这样巨大的密钥量给密钥分配和密钥管理都带来了极大的困难。

（**2**）公钥密码体制的概念，会画出公钥密码技术示意图，分析公钥密码体制的优缺点。
采用非对称密码技术的每个用户都有一对密钥：一个是可以公开的(称为加密密钥或公钥)，可以像　　号码一样进行注册公布；另一个则是秘密的(称为秘密密钥或解密密钥或私钥，它由用户严格保密保存)。它的主要特点是将加密和解密能力分开，因而可以实现多个用户加密的信息只能由一个用户解读，或由一个用户加密的信息而多个用户可以解读。前者可以用于公共网络中实现通信保密，而后者可以用于实现对用户的认证。
下图是公钥密码技术示意图。在图 4-4 中，E(eB，m)表示使用用户 B 的公开密钥 eB 对明文 m 进行加密，D(dB，c)表示使用用户 B 自己保存的秘密密钥 dB 对密文 c 进行解密。

4、考试范围
第四章：密码技术
（**3**）知道对称密码体制常用算法（置换、**DES**、**3DES**）、非对称密码体制常用算法（**RSA**）。
置换法
凯撒算法的推广是移动 K 位。单纯移动 K 位的置换算法很容易被破译，比较好的置换算法是进行映像。例如，将 26 个字母映像到另外 26 个特定字母中，如下表所示,利用置换发可将 attack 加密，变换为 QZZQEA。
加密算法要达到的目的（通常称为 DES 密码算法要求）主要为以下四点：
①提供高质量的数据保护，防止数据未经授权的泄露和未被察觉的修改。
②具有相当高的复杂性，使得破译的开销超过可能获得的利益，同时又要便于理解和掌握。
③ DES 密码体制的安全性应该不依赖于算法的保密,其安全性仅以加密密钥的保密为基础。
④实现经济，运行有效，并且适用于多种完全不同的应用。
DES 主要采用替换和移位的方法加密。
DES 算法的入口参数有三个：Key、Data、Mode。其中 Key 为 8 个字节共 64 位，是 DES 算法的工作密钥；Data 也为 8 个字节 64 位，是要被加密或被解密的数据；Mode 为 DES 的工作方式，有两种：加密或解密。
DES 算法是这样工作的：如 Mode 为加密，则用 Key 去把数据 Data 进行加密， 生成 Data 的密码形式（64 位）作为 DES 的输出结果；如 Mode 为解密，则用 Key 去把密码形式的数据 Data 解密，还原为 Data 的明码形式（64 位）作为 DES 的输出结果。在通信网络的两端，双方约定一致的 Key，在通信的源点用 Key 对核心数据进行 DES 加密，然后以密码形式在