物联网技术导论（第 3 版）

习题解答

（参考答案 V1.1）

仅供参考

西安交通大学 桂小林 编著

清华大学出版社

习题解答目录

物联网技术导论（第 3 版）.....1
第 1 章 绪论.....3
第 2 章 物联网体系结构.....6
第 3 章 传感与检测技术.....9
第 4 章 标识与定位技术.....12
第 5 章 物联网通信技术.....17
第 6 章 物联网数据处理.....23
第 7 章 物联网信息安全.....27
第 8 章 物联网典型应用.....32

第1章 绪论

一、选择题（单选或多选）

1、《未来之路》的作者是： B. 比尔·盖茨

2、智慧地球的提出者是： C.彭明盛

3、产品电子编码（Electronic Product Code，EPC）是由如下机构最早提出的：A.麻省理工学院

4、2009年8月7日，时任国务院总理在无锡微纳传感网工程技术研发中心视察时提出了：A.感知中国

5、2015年3月5日，时任总理在全国两会上作《政府工作报告》时首次提出：C.中国制造2025

6、RFID系统中，无源标签的能耗从何而来： B.磁场

7、下面不属于物联网感知技术的是： D.蓝牙

8、目前流行的智能手机的计步功能主要通过如下传感器实现：A.加速度

9、物联网的英文缩写为（）。 B、IoT

10、中国智能制造的典型创新性成果包括：

A.空中造楼机 B.穿隧道架桥机 C.隧道掘进机

二、简答题

1. 什么是物联网？物联网中的“物”主要指什么？

答：答：物联网是通过使用射频识别RFID(Radio Frequency Identification)、传感器、红外感应器、全球定位系统、激光扫描器等信息采集设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络。在物联网中，“物”的涵义除了电子产品外，还包括食物、服装、零部件和文化用品等非电子类物品。

2. 简述物联网的主要特征和每个特征的具体含义。

答：物联网具有全面感知、可靠传递、智能处理和深度应用四个主要特征。

3. 什么是RFID？什么是EPC？简述EPC和RFID的关系。

答：RFID是射频识别（Radio Frequency Identification）的缩写。EPC是产品电子编码 （Electronic Product Code)。RFID使用的编码技术是EPC，二者相互关联。

4. 简述物联网的起源。

答；物联网的起源可以追溯到1995年。比尔·盖茨在《未来之路》一书中对信

息技术未来的发展进行了预测。

5. 试述物联网的国内外发展现状。

答：2005年，国际电信联盟ITU发布《ITU互联网研究报告2005：物联网》，描述了网络技术正沿着“互联网—移动互联网—物联网”的轨迹发展，指出无所不在的“物联网”通信时代即将来临，信息与通信技术的目标已经从任何时间、任何地点连接任何人，发展到连接任何物品的阶段，而万物的连接就形成了物联网。

6. 分析物联网发展过程中所面临的主要问题和可采取的措施。

答：目前，尽管物联网的发展方兴未艾，但还有一系列问题需要解决，如政策、标准、安全、技术和商业模式等。

7. 简述物联网技术的主要应用领域，并举出几个实例。

答：物联网发展到今天，已经无时无刻充斥在我们的生活中。从二维条形码支付、刷卡乘车、不停车收费、手机导航和计步等，无不跟物联网技术密切相关。

8. 利用物联网技术，设计一种智能物流的解决方案。

答：智能物流解决方案的核心在于利用物联网技术实现物流过程的智能化、自动化和高效化管理。 通过物联网技术，可以实现对物流各个环节的实时监控、数据采集和智能分析，从而提高物流效率，降低成本，增强竞争力。

9. 什么是工业4.0？简述工业4.0的主要特征。

答：第四次工业革命的核心是物联网，其目标就是实现虚拟生产和与现实生产环境的有效融合，提高企业生产率。

10. 简述四次工业革命的发展历程。

答：第一次工业革命是1760-1840年的“蒸汽时代”；第二次工业革命是1840-1950年的“电气时代”；第三次工业革命是二战之后开创的“信息时代”；第四次工业革命是1998年之后的物联网时代。进入二十一世纪，人类面临空前的全球能源与资源危机、全球生态与环境危机、全球气候变化危机的多重挑战，由此引发了第四次工业革命——绿色工业革命。物联网技术的出现开创了第四次工业革命。第四次工业革命的核心是“人-机-物”深度融合。

11. 什么是中国制造2025？其提出的目标是什么？

答：《中国制造2025》是由国务院于2015年5月印发的部署全面推进实施制造

强国的战略文件，是中国实施制造强国战略第一个十年的行动纲领，对国家的工业制造现代化产生了深远影响。

12. 简述物联网、云计算、大数据和人工智能的相互关系。

答：物联网是数据获取的基础，云计算是数据存储的核心，大数据是数据分析的利器，人工智能是反馈控制的关键。物联网、云计算、大数据和人工智能构成了一个完整的闭环控制系统，将物理世界和信息世界有机融合在一起。

第2章 物联网体系结构

一、选择题

1. 三层的物联网体系结构不包括（ D ）。
2. 四层的物联网体系结构中，定位技术属于（ A ）。
3. 四层的物联网体系结构中，云计算技术属于（ C ）。
4. Zigbee是属于（ A ）中的标准协议。
5. RFID是属于（ B ）中使用的核心技术。
6. 下面属于M2M系统架构的是（BCD）。
7. 在无线传感器网络中，负责接入主干网络的节点是（ B ）。
8. 远程监控大坝水位，并根据水位远程控制泄洪的技术是（ B ）。
9. 人类从书桌上拿取一本书的过程属于（ B ）。
10. 人们按下电源开关开灯的过程属于（ A ）。

二、问答题

1. 什么是体系结构？简述体系结构对计算机系统的发展影响。

答：体系结构（Architecture）描述一组部件以及部件之间的联系。

体系结构与系统软件、应用软件、程序设计语言的紧密结合与相互作用也使今天的计算机与以往有很大的不同，并触发了大量的前沿技术，如物联网、云计算和大数据等。

2. 什么是物联网体系结构？研究物联网体系结构重点关注哪些因素？

答：物联网体系结构是指描述物联网部件组成和部件之间的相互关系的框架和方法。

3. 简述物联网体系结构的设计原则。

答：用户中心原则、时空关联原则、互联互通原则、开放共享原则、安全可靠原则等。

4. 分析三层物联网体系结构和四层物联网体系结构的差别和联系。

答：在物联网的4层体系结构中，数据处理层和应用决策层可以合二位一，称之为应用决策层，这样物联网四层体系结构就变成了三层体系结构，即感知控制层、数据传输层、应用决策层。

5. 简述四层物联网体系结构中每一层的功能。

答：（1）感知控制层是物联网发展和应用的基础，包括条形码识别器、各种类型传感器（如温湿度传感器、视频传感器、红外探测器等）、智能硬件（如电表、空调等）、和接入网关等。（2）数据传输层负责接收感知层数据，传输到数据处理层，并将数据处理结果返回感知层。（3）数据处理层提供物联网资源的初始化，监测资源的在线运行状况，协调多个物联网资源（计算资源、通信设备和感知设备等）之间的工作，实现跨域资源间的交互、共享与调度，实现感知数据的语义理解、推理、决策以及提供数据的查询、存储、分析、挖掘等。（4）应用决策层利用经过分析处理的感知数据，为用户提供多种不同类型的服务，如检索、计算和推理等。

6. 什么是EPC系统？简述EPC系统的组成。

答：电子产品编码(Electronic Product Code，EPC)的核心思想是为每一个产品提供唯一的电子标识符，通过射频识别技术实现数据的自动标识和采集。EPC系统由EPC编码体系、射频识别系统和信息网络系统三部分组成。

7. 什么是无线传感器网络？简述无线传感器网络的组成。

答：无线传感器网络(WSN)是由大量的密集部署在监控区域的智能传感器节点构成的一种网络应用系统。无线传感器网络系统是由大量功能相同或不同的无线传感器节点、接收发送器(sink)、Internet或通信卫星、任务管理节点等部分组成的一个多跳的无线网络。

8. 什么是CPS？简述CPS的组成。

答：息物理融合系统(Cyber Physical System，CPS)是一个综合计算、网络和物理环境的多维复杂系统，通过3C——计算(computation)、通信(communication)和控制(control)技术的有机融合与深度协作，实现大型系统的实时感知和动态控制。CPS分为四层：节点层、网络层、资源层和服务层。

9. 什么是M2M？简述M2M系统的组成。

答：M2M的定义可以分为广义和狭义两种。广义上的M2M包括Machine to Machine、Man to Machine以及Machine to Man，它是指人与各种远程设备之间的无线数据通信。狭义上的M2M是Machine to Machine的简称。

10. 什么是反馈控制？简述反馈控制在物联网中的应用。

答：反馈控制就是闭环控制。它是按偏差进行控制的，其特点是不论什么原

因使被控量偏离期望值而出现的偏差时，必定会产生一个相应的控制作用去减小或消除这个偏差，使被控量与期望值趋于一致。与传统反馈控制系统相比，物联网反馈控制建立在互联网络之上，对被控对象的通信链条更长，面临的安全问题更加复杂。

11. 简述物联网反馈控制的原理。

答：与传统自动控制系统相比，物联网建立在互联网络之上，同时需要区分不同的被控对象，因此更加复杂，控制系统的表现更加多样，计算机可以实现的各种控制也更加灵活。但是，由于网络是连接各个部件的途径，因此控制的结果具有很强的不确定性。所以，物联网控制系统的控制特性与传统的控制系统的控制特性有较大区别。

第3章 传感与检测技术

一、选择题

1.在传感检测模型中，负责将敏感元件输出转换成适于传输的电信号的元件是（ A ）。

2. 在传感检测模型中，负责将微弱(毫伏级)进行放大或调制的电路是(B)。

3. 在传感检测模型中，负责将电信号转换为数字信号的电路是（ D ）。

4. 下列不属于按传感器的工作原理进行分类的传感器是（ B ）。

5. 传感器的静态特性指标包括（ A ）。

6. 能够检测1500摄氏度以上高温的传感器是（ C ）。

7. 能够检测-200摄氏度低温的传感器是（ A ）。

8. 用遥控器控制电视机就是传感器把光信号转化为电信号的过程。下列采用同类传感器的应用是（ A ）。

9. 关于CCD和CMOS的优缺点的描述错误的是（ D ）。

10. 目前流行的智能手机的计步功能，主要通过（ A ）传感器实现。

二、问答题

1.什么叫传感器？它由哪几部分组成？它们的相互关系如何？

答：传感器是能感受规定的被测量并按照一定的规律转换成可用输出信号的器件或装置。通常，传感器由敏感元件和转换元件组成。其中，敏感元件是指传感器中能直接感受或响应被测量的部分；转换元件是指传感器中能将敏感元件感受或响应的被测量转换成适于传输或测量的电信号部分。 敏感元件的输入是被测的非电量，如温度、压力、位移、加速度等，敏感元件的输出就是转换元件的输入，转换元件的输出是电量，如电压、电流、电容、电阻等，输出信号的形式由传感器的原理确定。比如在金属电阻应变式传感器中，应变片是敏感元件，电阻丝是转换元件。由于传感器输出信号一般都很微弱，需要有信号调理与转换电路，进行放大、运算调制等， 信号调理转换电路以及传感器的工作必须有辅助的电源， 因此信号调理转换电路以及所需的电源都应作为传感器组成的一部分。

2.什么是传感器的静态特性？它有哪些性能指标？如何用公式表征这些性能指标？

答：传感器的静态特性是指被测量的值处于稳定状态时输出与输入的关系。如果被测量是一个不随时间变化，或随时间变化缓慢的量，可以只考虑其静态特性， 这时传感器的输入量与输出量之间在数值上一般具有一定的对应关系，关系式中不含有时间变量。对静态特性而言，传感器的输入量x与输出量y之间的关系通常可用一个如下的多项式表示： $y=a0+a1x+a2x2+\cdots+anxn$ 式中：a0——

输入量 x 为零时的输出量；a1，a2，…，an—— 非线性项系数。 各项系数决定了静态特性曲线的具体形式。传感器的静态特性一般用下述 5 个性能指标来描述，如灵敏度、 迟滞、线性度、重复性等。

3. 根据工作原理，可以将传感器分为哪几类？

答：传感器是实现自动检测和自动控制的首要环节，如果没有传感器对原始参数进行精确可靠的测量，那么无论是信号转换或信息处理，获取、显示最优化数据，进而实现精确控制都是不可能实现的。传感器一般是根据物理学、化学、生物学等特性、规律和效应设计而成的，其种类繁多，往往同一种被测量可以用不同类型的传感器来测量，而同一原理的传感器又可测量多种物理量，根据工作原理分类，将物理和化学等学科的原理、规律和效应作为分类依据，如电压式、热电式、电阻式、光电式、电感式等；

4.什么是应变效应？利用应变效应解释金属电阻应变片的工作原理。

答：金属电阻应变片的工作原理是吸附在基体材料上应变电阻随机械形变而产生阻值变化的现象，俗称为电阻应变效应。以金属丝应变电阻为例，当金属丝受外力作用时，其长度和截面积都会发生变化，从上式中可很容易看出，其电阻值即会发生改变，假如金属丝受外力作用而伸长时，其长度增加，而截面积减少，电阻值便会增大。当金属丝受外力作用而压缩时，长度减小而截面增加，电阻值则会减小。只要测出加在电阻的变化（通常是测量电阻两端的电压），即可获得应变金属丝的应变情。

5. 电感式传感器有几种结构形式？各有什么特点？

答：电感式传感器是利用线圈自感或互感系数的变化来实现非电量电测的一种装置。利用电感式传感器，能对位移、压力、振动、应变、流量等参数进行测量，它具有结构简单、灵敏度高、输出功率大、输出阻抗小、抗干扰能力强及测量精度高等一系列优点，因此在机电控制系统中得到广泛的应用。电感式传感器种类很多，根据感知原理可分为自感式、互感式和电涡流式等。习惯上讲的电感式传感器通常指自感式传感器，而互感式传感器由于是利用变压器原理，又往往做成差动形式，所以常被称为差动变压器式传感器。

6. 石英晶体的 x、y、z 轴的名称及特点是什么？

答：天然结构石英晶体的理想外形是一个正六面晶柱，晶体学中它可用三根互相垂直的轴来表示，其中纵向轴Z称为光轴；经过正六面体棱线并垂

直于光轴的X轴称为电轴；与X轴和Z轴同时垂直的Y轴（垂直于正六面体的棱面）称为机械轴。通常把沿电轴X方向的作用力下产生电荷的压电效应称为“纵向压电效应”，而把沿机械轴Y方向的作用力下产生电荷的压电效应称为“横向压电效应”，沿光轴Z方向受力则不产生压电效应。

7. 简述变磁通式和恒磁通式磁电传感器的工作原理。

答：恒磁通式磁电传感器由永久磁铁、线圈、弹簧、金属骨架等组成。当恒通式磁电传感器工作时，传感器与被测物体紧固在一起，当物体振动时，传感器外壳也随之振动。变磁通式磁电传感器的线圈和磁铁部分静止不动，与被测物连接而运动的部分是用导磁材料制成的。在运动中，它们改变磁路的磁阻，因此改变穿过线圈的磁通量，于是在线圈中就会产生感应电动势。

8. 测量位移的传感器有哪些？简述其工作原理。

答：应变电阻器可用来测量位移；电涡流式传感器能测量位移。

9. 智能传感器可分为哪几类？其特点是什么？

答：从结构上划分，智能传感器可以分为集成式、混合式和模块式。集成智能传感器是将一个或多个敏感器件与微处理器、信号处理电路集成在同一硅片上，集成集成度高，体积小，但目前的技术水平还很难实现；将传感器和微处理器、信号处理电路做在不同芯片上，则构成混合式智能传感器，目前这类结构较多；初级的智能传感器也可以由许多互相独立的模块组成，如将微计算机、信号调理电路模块、数据电路模块、显示电路模块和传感器装配在同一壳结构内则组成模块式智能传感器。

智能传感器具有以下三个优点：通过软件技术可实现高精度的信息采集，而且成本低；具有一定的编程自动化能力；功能多样化。

10. 简述智能集成温度传感器DS18B20的原理和功能。

答：DS18B20是一款单总线的智能型集型的数字温度传感器，具有体积小，硬件开销低，抗干扰能力强，精度高的特点。DS18B20数字温度传感器接线方便，只需要一条数据线和一条地线即可与处理器进行数据传输，并提供9~12位摄氏温度测量数据。

第4章 标识与定位技术

一、选择题

1．1977年，欧洲共同体在12位UPC-A码的基础上，开发出与UPC码兼容的（ B ）码。

2. 建立全球统一标识系统，促进国际贸易的机构是协调全球统一标识系统在各国的应用，确保成员组织规划与步调的充分一致的机构是（ A ）。

3．在中国大陆，EAN -13厂商识别代码由（ A ）位数字组成，由中国物品编码中心负责分配和管理。

4. 编码方式属于模块组配编码法的码制是（ D ）

5. 关于二维条形码，以下说法正确的是（ A ）

6. 使用微信对商家提供的二维条形码进行扫码付款，该扫描过程属于（B）

7. 使用手机扫描QR二维条形码的原理是基于（ C ）。

8. RFID系统中，无源标签的能耗从何而来（ B ）

9．在RFID系统中，一般采用（ D ）法来解决碰撞。

10．在铁路机车车号识别系统中，安装在铁轨中间的是（ C ）。

11．在基本二进制算法中，为了从N个标签中找出唯一一个标签，需要进行多次请求，其平均次数L为（ B ）。

12. 在纯ALOHA算法中，假设电子标签在t时刻向阅读器发送数据，与阅读器的通信时间为T0，则碰撞时间为（ A ）。

13.（ B ）是电子标签的一个重要组成部分，它主要负责存储标签内部信息，还负责对标签接收到的信号以及发送出去的信号做一些必要的处理。

14. 空间定位系统的设计方案中通常包括（ B ）部分、地面监控部分和用户接收部分。

15．移动终端实施空间定位最少需要接收（ C ）导航卫星的信号。

二、简单题

1. 简述一维条码的分类以及编码方式。

答：世界上常用的一维条形码有EAN条形码、UPC条形码、25条形码、交叉25条形码、库德巴条形码、Code 39条形码和Code 128条形码等。

2. 简述UPC与EAN码的应用。

答：零售业、图书馆、仓储管理与物流跟踪、质量跟踪管理等。

3. UPC和EAN的共同符号特征有哪些？

答：UPC码(Universal Product Code)是美国统一代码委员会制定的一种商品用条码，主要用于美国和加拿大地区，我们在美国进口的商品上可以看到。UPC码是最早大规模应用的条码，其特性是一种长度固定、连续性的条码，由于其应用范围广泛，故又被称万用条码。 UPC码仅可用来表示数字，故其字码集为数字0~9。UPC码共有A、B、C、D、E等五种版本，不同版本对应各自不同的应用对象。EAN码是国际物品编码协会制定的一种商品用条码，通用于全世界。EAN码符号有标准版（EAN-13）和缩短版（EAN-8）两种标准版表示13位数字，又称为EAN-13码，缩短版表示8位数字，又称EAN-8。

4. 假设编码系统字符为“0”，厂商识别代码为012320，商品项目代码为0007，试将其表示成UPC-E形式。

答：在特定条件下，12位的UPC-A条码可以被表示为一种缩短形式的条码符号，即UPC-E条码。 

5. 行排式二维条码与矩阵式二维条码的编码原理有何不同？

答：二维码可以分为堆叠式/行排式二维码和矩阵式二维码。堆叠式/行排式二维码形态上是由多行短截的一维条码堆叠而成；矩阵式二维码以矩阵的形式组成，在矩阵相应元素位置上用“点”表示二进制“1”， 用“空”表示二进制“0”,“点”和“空”的排列组成代码。

6. 试对数字 0123456789012345(16 个数字字符)进行编码，生成 QR 码。

答：QR 码的编码过程主要包括数据分析、数据编码、纠错编码、构造矩阵、掩模和格式及版本信息配置等。

（1）进行数字分组，每 3 位一组，即“012 376 54”;

（2）将“012 376 54”中按 3 位一组依次转换成 10 位二进制，例如，012 转换为 0000001100；376 转成 0101111000；54 转换成 0110110。

（3）将字符个数“8”转成二进制，即 0000001000;

（4）在二进制系列前加入模式指示符 0001，得 0001 0000001100 0101111000 0110110。

7. 什么是 RFID 技术？RFID 系统的基本组成部分有哪些？RFID 工作原理是什么？

答：RFID(射频识别：Radio Frequency Identification)是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取相关数据，识别工作无须人工干预，作为条形码的无线版本，RFID技术具有条形码所不具备的防水、防磁、耐高温、使用寿命长、读取距离大、标签上数据可以加密、存储数据容量更大、存储信息更改自如等优点，其应用将给零售、物流等产业带来革命性变化。RFID系统是由射频标签、识读器和计算机网络组成的自动识别系统。通常，识读器在一个区域发射能量形成电磁场，射频标签经过这个区域时检测到识读器的信号后发送存储的数据，识读器接收射频标签发送的信号，解码并校验数据的准确性以达到识别的目的。

8. 什么是电子产品代码标签？

答：电子产品代码是与全球标准代码条形码相对应的射频技术代码。电子产品代码是由一系列数字组成，能够辨别具体对象的生产者，产品、定义，序列号。

9. RFID 系统的工作频率有哪些？

答：根据读写器发送无线信号所工作的频率可划分为：低频(30~300kHz)、高频(3~30MHz)、超高频(300MHz~3GHz)与微波频段2.45GHz~5.8GHz)。低频系统一般工作在100~500kHz，常见的工作频率有125kHz、134.2kHz；高频系统工作在10~15MHz，常见的高频工作频率为13.56MHz；超高频工作频率为850~960MHz，常见的工作频率为915MHz；微波工作在2.4~5GHz的微波频段。低频系统用于短距离、低成本的应用，如多数的门禁控制、动物监管、货物跟踪；高频系统用于门禁控制和需传送大量数据的应用；超高频系统应用于需要较长的读写距离和较高的读写速度的场合，如火车监控、高速公路收费系统等。

10. 什么叫标签碰撞和读写器碰撞？常见的标签碰撞和读写器碰撞有哪些？

答：在RFID系统应用中，存在多个读写器或多个标签，因而造成的读写器之间或标签之间的相互干扰，统称为碰撞。在RFID系统中存在两种类型的通信碰撞：第一种：阅读器碰撞是指多个阅读器同时与一个标签通信，致使标签无法区分阅读器的信号，导致碰撞的发生；第二种：电子标签碰撞是指多个标签同时响应阅读器的命令而发送信息，引起信号碰撞，使阅读器无法识别标签；由于阅读器能检测碰撞并且阅读器之间能相互通信，所以阅读器碰撞能很容易得到解决。因而，射频识别系统中的碰撞一般是指电子标签碰撞。

11. 未来RFID标签能否取代条码技术？

答：RFID和条码技术各有其应用场景，未来RFID不会代替条码技术。

12.全球卫星定位系统由哪几部分组成？每一部分的功能是什么？

全球卫星定位系统由三部分组成：空间部分即GPS星座；地面控制部分即地面监控系统；用户设备部分即GPS 信号接收机。

13. 蜂窝定位技术与卫星定位技术的异同点有哪些？

答：蜂窝定位（即基站定位）技术的原理为：移动电话测量不同基站的下行导频信号，得到不同基站下行导频的TOA（Time of Arrival，到达时刻）或TDOA(Time Difference of Arrival，到达时间差)，根据该测量结果并结合基站的坐标，一般采用三角公式估计算法，就能够计算出移动电话的位置。同：两者都是利用时间差原理。异：一个利用卫星，一个利用基站。

14. 蜂窝定位技术的常用方法有几种？试简述每一种方法的基本原理。

答：（1）蜂窝小区COO（Cell of Origin）定位是一种单基站定位，是通过手机当前连接的蜂窝基站的位置进行定位的。（2）基于电波传播时间TOA (Time of Arrival)的定位是以一种三基站定位方法。该定位方法以电波的传播时间为基础，利用手机与三个基站之间的电波传播时延，通过计算得出手机的位置信息。（3）基于电波到达时差TDOA（Time Difference of Arrival）定位与TOA定位类似，也是一种三基站定位方法。该方法是利用手机收到不同基站的信号时差来计算手机的位置信息的。（4）到达角度AOA(Angle of Arrival)定位是一种两基站定位方法，它根据信号的入射角度进行定位。该方法是假定基站可以测量出手机发射信号到达基站的角度，如果手机和基站处于可视范围内，则利用手机分别与两个基站的夹角，两条射线的交点就是手机的位置。

15. 简述WiFi定位的两种常用方法及其工作原理。

答：WiFi 定位的两种常用方法包括三角定位法和指纹定位法。

三角定位法是一种基本的 WiFi 定位技术。它通过测量设备与三个或更多 WiFi 热点之间的信号强度，然后利用三角测量原理计算出设备的位置。这种方法计算简单，但需要至少三个已知位置的 WiFi 热点。其工作原理基于信号强度的测量，当设备靠近某个 WiFi 热点时，接收到的信号强度会增强，而远离该热点时，信号强度会减弱。通过测量设备与多个 WiFi 热点之间的信号强度，可以计算出设备的位置。

指纹定位法是一种更先进的 WiFi 定位技术。它通过收集大量 WiFi 热点的信号强度数据，形成一个“指纹”数据库。当需要定位时，设备测量其周围的 WiFi 热点信号强度，并与指纹数据库进行匹配，从而确定设备的位置。这种方法准确性较高，但需要大量的数据收集和处理。其工作原理依赖于预先收集的 Wi-Fi 指纹数据，这些数据包括不同位置上的 Wi-Fi 信号强度信息。通过将这些信息与实时测量的信号强度进行匹配，可以估计设备的位置。

第5章 物联网通信技术

一、选择题

1. WIFI和4G这两种技术的关系本质上是（ A ）
2. 802.11b最大的数据传输速率可以达到（ D ）
3. 802.11g最大的数据传输速率可以达到（ B ）
4. 802.11n可以加入的标准不包括（ A ）
5. WIFi接入点AP的主要功能为（ A ）
6. 在Zigbee技术中，PHY层和MAC层采用（ A ）协议标准。
7. 在Zigbee技术中，PHY层物理层的数据传输速率为（ C ）。
8. 192.168.1.1代表的是（ C ）地址。
9. 对于一个没有见过子网划分的传统C类网络来说，允许安装的最多主机数为（C）。
10. IP地址219.55.23.56的缺省子网掩码有（ C ）位。
11. 保留给用户自测试I类地址是（ B ）。
12. 在TCP/IP协议栈的数据发送过程中，报文是由（ B ）组装完成的。

二、问答题

1. 近距离无线通信技术有哪些？各有什么特点？

答：近距离无线通信技术有蓝牙(Bluetooth)、无线局域网802.11(Wi-Fi)、红外数据传输(IrDA)、ZigBee、WiMax、超宽频(Ultra WideBand)、短距通信(NFC)、WiMedia、GPRS、EDGE、无线1394等。它们都有其立足的特点，或基于传输速度、距离、耗电量的特殊要求；或着眼于功能的扩充性；或符合某些单一应用的特别要求;或建立竞争技术的差异化等。

2. WiFi的常用组网方式有哪些？

答：WIFI的常用组网方式可分为三类：桥接型WIFI、路由型WIFI、集中控制型WIFI。从WIFI的应用环境来看，WIFI可分为室内型WIFI和室外型WIFI，依据应用方式和发射功率又可进一步作细分。

3. 简述蓝牙的组网特点。

答：蓝牙技术是一种低成本、短距离的无线个人网络传输(WireleSS Personal Area Network)技术，其主要目标是提供一个全世界通行的无线传输环境，以通过无线电波来实现所有移动设备之间的信息传输服务。蓝牙模块组网技术的主要特点如下：

(1)支持移动联网。用户可以像使用移动电话那样灵活的移动计算设备的位置，而使设备仍然保持持续的网络连接。

(2)不需要使用物理线路，安装非常简便，成本低、体积小，可用于更多的设备。

(3)网络使用的高频电波可以穿透墙壁或玻璃窗，所以设备可以在有效范围任意放置。

(4)多层安全防护措施可以确保用户隐私。

(5)改动网络结构或布局时，不需要对网络进行重新设置。

4. 简述ZigBee的组网特点。

答：Zigbee是IEEE 802.15.4协议的代名词。根据这个协议规定的技术是一种短距离、低功耗的无线通信技术。主要特点如下：① 自动组网，网络容量大。② 网络时延短。③ 模块功耗低，通讯速率低。④ 传输距离可扩展。⑤ 成本低。⑥ 可靠性好，安全性高。

5. 按照ISO的网络体系结构标准，WiFi、蓝牙以及ZigBee分别工作在哪些层？

答：Wifi、蓝牙和zigbee分别属于数据链路层和物理层。Zigbee和Wifi是802.15和802.11的技术标准。802.11主要是针对局域网的相关标准。而局域网是工作在OSI数据链路层和物理层的，其中蓝牙和zigbee属于物理层设备。

6. 远距离无线通信技术有哪些？各有什么特点？

答：远距离无线通信技术有卫星、微波。

7. 卫星的工作方式及常用频段是什么？

答：UHF（Ultra High Frequency）或分米波频段，频率范围为300MHz-3GHz。该频段对应于IEEE的UHF（300MHz-1GHz）、L（1-2GHz）、以及S（2-4GHz）频段。UHF频段无线电波已接近于视线传播，易被山体和建筑物等阻挡，室内的传输衰耗较大。

SHF（Super High Frequency）或厘米波频段，频率范围为3-30GH。该频段对应于IEEE的S（2-4GHz）、C（4-8GHz）、Ku（12-18GHz）、K（18-27GHz）以及Ka（26.5-40GHz）频段。分米波，波长为1cm-1dm，其传播特性已接近于光波。

EHF（Extremly High Frequency）或毫米波频段，频率范围为30-300GHz。该频段对应于IEEE的Ka（26.5-40GHz）、V（40-75GHz）等频段。发达国家已开始计划，当Ka频段资源也趋于紧张后，高容量卫星固定业务（HDFSS）的关口站将使用50/40GHz的Q/V频段。

8. 4G与5G的主要区别是什么？

答：4G与5G的主要区别在于速度、延迟、容量、覆盖范围、频谱效率和应用场景等方面。

速度方面。5G网络的传输速度远高于4G，理论上5G的下载速度可以达到10Gbps，而4G的下载速度通常在100Mbps左右。

延迟方面，5G网络具有极低的延迟，可以达到毫秒级甚至更低，而4G网络的延迟通常在几十毫秒到几百毫秒之间。

容量方面，5G网络比4G网络能够连接更多的设备，支持更高的数据传输量。5G网络每平方公里可以连接数百万个设备，而4G网络则相对较少。

在覆盖范围上，5G网络虽然速度更快，但由于使用高频谱，其覆盖范围相对较小，需要在更靠近基站的地方才能连接到5G网络，而4G网络的覆盖范围更广泛。不过，随着5G基站的逐渐建设和优化，5G网络的覆盖范围也会逐渐扩大。

频谱效率方面，5G的频谱效率比4G高，能够提供更大的带宽和更快的传输速率。5G使用低频、中频和毫米波频段，而4G主要使用低频谱。

应用场景方面，5G的高速度和低延迟特性使其适用于更多应用场景，如自动驾驶、远程医疗、虚拟现实和增强现实等。而4G网络主要侧重于提供基本的互联网连接和数据处理。

9. 有线通信技术有哪些？

答：有线通信技术是一种通信方式，狭义的现代有线通信是指有线电信，即利用金属导线、光纤等有形媒质传送信息的方式。光或电信号可以代表声音，文字，图像等。有线通信包括光纤、双绞线、同轴光缆等等。

10. 光纤通信原理是什么？

答：光纤通信是采用光纤作为介质传播信号的，在长距离传播上会采用光缆（也就是把很多光纤集中在一起加上保护套管），发射信号的为高速激光器，根据送来的电信号来调制发光，然后将忽强忽弱的光送入到光纤中传输，传输的原理是光的全反射。接收信号的为光敏器件，根据来光的强弱把光信号还原为0或1的电信号。

11. 以太网的特点及组网方式是什么？

答：以太网(Ethernet)指的是由Xerox公司创建并由Xerox、Intel和DEC公司联合开发的基带局域网规范，是当今现有局域网采用的最通用的通信协议标准，是目前应用最广泛的一类局域网。以太网采用一种称为载波监听多路访问/冲突检测CSMA/CD(Carrier Sense Multiple Access/Collision Detection)的共享访问方案，即多个工作站都连接在一条总线上，所有的工作站都不断向总线上发出监听信号，但在同一时刻只能有一个工作站在总线上进行传输，而其它工作站必须等待其传输结束后再开始自己的传输。早期的网络是总线型的组网方式，随着技术进步，组网方式包括星型、环型等。

12. Internet 的 TCP/IP 协议栈结构是什么？

答：Inetent的TCP/IP分为4层：链路层，网络层，传输层，应用层。

13. 以 FTP 为例，解释网络各层的工作原理及包结构。

答：FTP目标是提高文件的共享性，提供非直接使用远程计算机，使存储介质对用户透明和可靠高效地传送数据。FTP可完成两台计算机之间的拷贝，从远程计算机拷贝文件至自己的计算机上，称之为“下载（download)”文件。若将文件从自己计算机中拷贝至远程计算机上，则称之为“上载（upload)”文件。在TCP/IP协议中，FTP标准命令TCP端口号为21，Port方式数据端口为20。FTP的传输有两种方式：ASCII传输模式和二进制数据传输模式。

14. IP 地址的类型有哪些？202.196.96.5 属于哪类 IP?

答：按照分类，有5类：

A类：前8位为网络号，后24位为主机号，网络号首位为0。(32位的二进制)

B类：前16位为网络号，后16位为主机号，网络号前两位为10。

C类：前24位为网络号，后8位为主机号，网络号前三位为110。

D类：前4位为1110，后面28位是多播组号。

E类：前5位为11110，后面27位保留。

其中ABC类为网络单播地址，D类为组播地址。E类保留留待后用。

202.196.96.5地址属于C类

15. 试述 IPv6 与 IPv4 的区别。

答：IPV6拥有更大的地址空间。IPv4中规定IP地址长度为32，即有2^32-1个地址；而IPv6中IP地址的长度为128，即有2^128-1个地址。
IPv6拥有更小的路由表。IPv6的地址分配一开始就遵循聚类(Aggregation)的原则，这使得路由器能在路由表中用一条记录(Entry)表示一片子网，大大减小了路由器中路由表的长度，提高了路由器转发数据包的速度。
增强的组播(Multicast)支持以及对流的支持(Flow-control)。

16. 常用网络互联设备及工作方式有哪些？

答：网络互联设备包括中继器/集线器。中继器是最简单的网络互联设备，主要完成物理层的功能，负责在两个节点的物理层上按位传递信息，完成信号的复制、调整和放大功能，以此来延长网络的长度。集线器在网络中只起到信号放大和重发作用，其目的是扩大网络的传输范围，而不具备信号的定向传送能力。网桥/交换机，是数据链路层设备，在局域网之间存储转发帧；通过地址过滤，有选择的转发信息帧。路由器在不同的网络之间存储转发分组（数据报文）。

17. 简述路由选择算法中的洪泛法的原理，并设计一种改进的选择性洪泛法。

答：洪泛法（Flooding）是一种简单的路由算法，其基本原理是：当一个数据包到达某一个节点时，该节点会将数据包复制并发送到所有可达的邻居节点，除了它从中接收到数据包的节点。 这种机制确保了网络中的每个节点都将接收到数据包，但也可能导致大量的重复数据包。
洪泛法的优点在于其实现简单，能够在没有固定网络结构或网络结构快速变化的环境中有效工作。然而，这种方法也会导致大量的重复数据包，特别是在大型或密集网络中，从而占用大量的网络资源，降低效率。
为了减少网络流量和防止无限循环，通常在洪泛法中引入了两种机制：设置合适的生存时间（TTL）值以保证数据包经过有限跳数，以及维护数据分组序号（SEQ）和路由表来进行重复分组检测。

18. 描述 IPv4 首部的结构，并说明其大小的计算方法。

答：IPv4 首部的结构包括多个关键字段，如版本、首部长度、区分服务、总长度等。

版本（Version）：由 4 比特构成，表示 IP 首部的版本号，IPv4 的版本号为 4。

首部长度（IHL: Internet Header Length）：由 4 比特构成，表明 IP 首部的大小，单位为 4 字节。没有选项时，首部长度为 20 字节；如果有选项，最大长度可达 60 字节。

区分服务（TOS: Type Of Service）：用于标识数据包的重要程度，实现服务质量（QoS）。

总长度（Total Length）：整个数据报的长度，单位为字节，最大可达 65535 字节。

标识（Identification）、标志（Flags）、片偏移量（Fragment Offset）：用于控制数据报的分片和重组。

生存时间（TTL: Time To Live）：数据报可以经过的最多路由设备数。

首部检验和（Header Checksum）：根据 IP 首部计算的检验和码，用于错误检测。

源 IP 地址和目的 IP 地址：指定发送方和接收方的地址。

IPv4 首部大小的计算方法如下：

首部长度字段的取值范围是 0101 到 1111，即十进制的 5 到 15。没有选项时，首部长度为 54 字节=20 字节；如果有选项，最大可达 154 字节=60 字节。

总长度 = 首部长度 + 数据载荷长度。例如，如果一个数据报的总长度为 1020 字节，首部长度为 20 字节，则数据载荷长度为 820 字节。

第6章 物联网数据处理

一、选择题

1.下列选项中，不属于大数据的特征是（ D ）。

2. 当图片的分辨率为1024*768，色彩为16位时，则该图片占用的存储空间为（ A ）。

3. 下列选项中，属于结构化数据的是（ D ）。

4. 下面选项中，属于文本数据的是（ B ）。

5. 从关系模式中找出满足给定条件的那些元组称为（ A ）。

6. 从关系模式中挑选若干属性组成新的关系称为（ B ）。

7. SQL中创建基本表的命令是（ C ）。

8. SQL中完成数据编辑功能的命令不包括（ A ）。

9. 分类的方法不包括 （ A ）。

10. 在HDFS中实施的副本策略中，（ B ）副本存在在同一服务器机架的不同节点上。

二、问题题

1. 物联网数据的主要特点有哪些？

答：物联网数据特点有海量Volume、多样 Variety、高速Velocity和价值密度低Value。

物联网应用中存在采样频率过高以及不同的感知设备对同一个物体同时感知等情况，这类情况导致了大量的冗余数据，所以相对来说数据的价值密度较低，但是只要合理利用并准确分析，将会带来很高的价值回报。

2. 数据预处理主要针对哪些数据？这些数据的特点是什么？

答：数据预处理常用的方法数据清洗（data cleaning）、数据集成（data integration）、数据转换（data transformation）和数据归约（data reduction）等。数据预处理主要针对结构型和非结构型数据。

3. 什么是知识？知识如何分类？

答：知识是指人们在实践中获得的认识和经验。按现代认知心理学的理解，知识有广义与狭义之分。广义的知识可以分为两类，即陈述性知识、程序性知识。

4. 数据挖掘的步骤是什么？什么是聚类分析？简述最大树聚类法。

答：关联规则挖掘过程主要包含两个阶段：第一阶段必须先从资料集合中找出所有的高频项目组(Frequent Itemsets)，第二阶段再由这些高频项目组中产生关联规则(Association Rules)。聚类分析又称集群分析，它是研究（样品或指标）分类问题的一种统计分析方法。最大树聚类法是模糊聚类方法的一种，目标是建立起相似系数构成的相似矩阵，然后以此构建基于模糊相似矩阵的最大树，最后利用λ-截集进行分类。

5. Hadoop可以用来做什么？它解决了目前应用场景中的什么问题？它存在什么缺点吗？

答：Hadoop是一个开源的框架，可编写和运行分布式应用处理大规模数据，是专为离线和大规模数据分析而设计的，并不适合那种对几个记录随机读写的在线事务处理模式。

6. 试构建HDFS文件系统，并编写代码实现文件的上传与下载。

答：略。

7. 试构建MapReduce运行环境，并编写代码实现对HDFS文件系统中文件的操作。

答：略。

8. 分析HDFS文件系统与数据库系统之间的区别。

答：文件系统和数据库系统之间的区别：

（1）文件系统用文件将数据长期保存在外存上，数据库系统用数据库统一存储数据；

（2）文件系统中的程序和数据有一定的联系，数据库系统中的程序和数据分离；

（3）文件系统用操作系统中的存取方法对数据进行管理，数据库系统用DBMS统一管理和控制数据；

（4） 文件系统实现以文件为单位的数据共享，数据库系统实现以记录和字段为单位的数据共享。

9. 简述文本检索技术的原理。

答：基于文字的检索主要根据文档的文字内容来计算查询和文档的相似度。这个过程通常包括查询和文档的表示及相似度计算，二者构成了检索模型。略

10.简述基于内容的图像检索技术的原理。

答：基于内容的图像检索（CBIR），即把图像的视觉特征，例如颜色、纹理结构和形状等，作为图像内容抽取出来，并进行匹配、查找。略

12.简述音频信号的检索方法。

答：音频特征有。⑴带宽(bandwidth)是指取样信号的频率值范围。⑵响度(loudness)是用分贝表示的短时傅里叶变化。⑶过零率(Zero-crossing Rate)是指在一个短时帧内，离散采样信号值由正到负和由负到正变化的次数，这个量大概能够反映信号在短时帧里的平均频率。

13. 什么是数据副本策略？数据副本策略主要解决云存储中的什么问题？

答：数据副本策略就是将副本存储到不同机架的机器上的策略。副本大致均匀地分布在整个集群中，可以有效防止因整个机架出现故障而造成的数据丢失，并且可以在读取数据时充分利用机架自身网络带宽。

14. 什么是数据去重技术?在云存储中使用数据去重技术有什么好处？

答：数据去重技术是一种消除冗余数据的技术。可以节约大量云存储空间，优化数据存储效率。目前，数据去重技术主要有数据压缩和冗余数据删除技术。

15. 试说明利用 MapReduce 快速统计一本书籍中不同单词数量的方法。

答：利用 MapReduce 快速统计一本书籍中不同单词数量的方法主要包括以下几个步骤：

首先，需要在 Windows 系统上安装 VMware 和 CentOS 镜像，通过 Xmanager 搭建一个 Hadoop 集群环境。

准备一个包含英语文章的文本文件（例如 word1.txt）。

安装 IDEA 或其他支持 Java 的集成开发环境。

创建三个 Java 类：Drive（运行类）、Map（实现 Map 过程）和 Reduce（实现 Reduce 过程）。

在 Map 类中，将文本按空格分割成单词，并输出每个单词及其计数。

在 Reduce 类中，对每个单词的计数进行汇总。

将编写好的代码编译成. jar 文件。
将. jar 文件上传到 Hadoop 集群中的主节点。
在 Hadoop 集群上启动 Hadoop 服务。
将输入文件上传到 HDFS 的指定目录。
运行 jar 包，指定输入和输出路径。
查看输出结果，得到每个单词的出现次数。
略。

第7章 物联网信息安全

一、选择题

1. 异常检测的方法不包括（ ）。

A. 基于模型的方法 B. 基于近邻的方法 C. 基于规则的方法 D. 基于密度的方法

2.下面属于生物特征识别的身份认证是（ B ）。

3. 信息如果只能由低安全级的客体流向高安全级的客体，高安全级的客体信息不允许流向低安全级的客体，则这个安全策略是（ A ）

4. 当一个组织（公司）的系统中有大量数据时，需要采用（ D ）手段来保护系统数据安全。

5. 对称加密算法DES是（A）的英文缩写。

6. 如果恺撒密码的密钥K=4，设明文为YES，则密文是（ B ）

7. RSA的公开密钥(n,e)和秘密密钥(n,d)中的e和d必须满足（ C ）。

8. 下面不是隐私保护的主要方法的是（ D ）。

9. 关于HASH描述准确的（ C ）

10. 防篡改技术不依赖于(A)技术。

二、简答题

1. 简述物联网安全问题和特征。

答：（1）已有的对传感网、互联网、移动网、安全多方计算、云计算等的一些安全解决方案在物联网环境中可以部分使用，但另外部分可能不再适用。（2）即使分别保证了感知控制层、数据传输层和应用层的安全，也不能保证物联网的安全。

2. 简述物联网面临的主要安全问题。

答：物联网作为一个人机物融合系统，面临的安全问题十分复杂，主要包括：物联网感知层安全问题、物联网传输层安全问题、物联网应用层安全问题等。

3. 简述物联网的感知层安全挑战和安全技术。

答：1）非法跟踪；2）中间人攻击；3）重放攻击；4）物理破解；5）伪造或克隆RFID标签；6）扰乱RFID标签信息读取；7）拒绝服务攻击；8）屏蔽攻击等。

4. 简述感知层的WSN安全机制和RFID安全机制。

答：为了保证RFID的隐私安全，防止隐私攻击，可以采用如下几大类RFID安全机制：改变关联性方法，改变唯一性方法，隐藏信息方法、无线隔离方法和同步方法。

5. 简述物联网传输层面临的安全问题及主要手段。

答：（1）信道开放带来的侦听问题。（2）终端管理不善带来的病毒、木马入侵问题。(3)安全协议存在漏洞的问题。(4)接入过程缺乏交互认证的问题。(5)互联网安全问题。

6. 简述密码学的基本概念和发展历程。

答：密码学包含两个互相对立的分支，即密码编码学（cryptography）和密码分析学（cryptanalytics)。前者编制密码以保护秘密信息，而后者则研究加密消息的破译以获取信息。二者相辅相成。密码学的发展史大致可以分为三个阶段：（1）在1949年之前，是密码发展的第一阶段，即古典密码体制，它只是一门艺术 ，而不是一门科学。（2）从1949年到1975年，是密码学发展的第二阶段。把密码学置于坚实的数学基础之上,标志着密码学作为一门学科的形成。(3)1976年，提出公开密钥，这是密码学的第三阶段。

7. 简述对称密码和非对称的密码的区别与联系。

答：密码模型可以分为对称密码系统和非对称密码系统。在对称密码系统中，加密密钥和解密密钥相同，或者一个密钥可以从另一个导出，能加密就能解密，加密能力和解密能力是结合在一起的，开放性差。在非对称密码系统中，加密密钥和解密密钥不相同，从一个加密密钥导出解密密钥是计算复杂的、困难的，加密过程和解密过程是分开的，开放性好，适合在网络上传播。

8. 什么是身份认证？身份认证有哪些方法和手段？

答：身份认证也称为“身份验证”或“身份鉴别”，是指在计算机及计算机网络系统中确认操作者身份的过程。常用的身份认证方法包括：口令、指纹、证书、刷脸等。

9. 什么是访问控制？常用的访问控制模型有哪几种？

答：访问控制就是在身份认证的基础上，依据授权对提出的资源访问请求加以控制。常用的访问控制模型有BLP访问控制模型、基于角色的安全访问控制模型和基于属性的安全访问控制模型等。

10. 什么是数字签名？数字签名主要解决什么问题?

答：数字签名是指用户用自己的私钥对原始数据的哈希摘要进行加密所得的数据。数字签名技术是保证信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的确定性的一种有效的解决方案。

11. 什么是隐私保护？位置隐私保护的主要方法有哪些？

答：隐私保护是指对敏感的数据进行脱敏保护的措施。隐私保护可以通过数据加密、数字水印、数据混淆、匿名等技术进行实现。

12. 简要说明数字签名的工作原理和应用场景。

答：数字签名的工作原理是通过使用私钥对原始数据进行加密生成签名，然后使用公钥对签名进行解密验证。具体步骤如下：

发送方使用哈希函数对消息进行哈希处理，得到消息摘要。

发送方使用私钥对消息摘要进行加密，得到数字签名。

发送方将消息和数字签名一同发送给接收方。

接收方使用相同的哈希函数对消息进行哈希处理，得到新的消息摘要。

接收方使用发送方的公钥对数字签名进行解密，得到解密后的消息摘要。

接收方比较两个消息摘要，若相同，则验证成功，证明数据未被篡改。

数字签名的应用场景非常广泛，主要包括：

电子商务：在电子商务中，数字签名用于确保订单、付款、物流等环节的安全性和真实性。

电子合同：通过数字签名，可以确保合同内容的完整性和真实性，防止篡改。

电子支付：在电子支付中，数字签名确保交易信息的真实性和完整性。

文件传输：在文件传输过程中，数字签名保护文件内容不被篡改，并验证文件的发送者身份。

网络通信：数字签名用于网络通信中的数据完整性保护和身份认证，提高通信的安全性。

13. 简述 DES 算法的工作原理。

答：DES 的工作原理为：DES 对 64 比特的明文数据 M 进行操作，M 经过一个初始置换 IP 后，将被分成左半部分 L_0 和右半部分 R_0，两部分都是 32 比特。在密钥 K_1 控制下对 R_0 进行轮函数 f 运算后，再与 L_0 异或，运算结果作为 R_1；而将 R_0 直接作为 L_1 的输入。由此得到第 2 轮的输入 L_1 和 R_1，以此类推，经过 16 轮相同运算后，得到 L_{16} 和 R_{16}。然后，交换左、右 32 比特为 R_{16} 和 L_{16}，合并为 64 比特

后经过一个逆置换 IP^{-1}，就产生了64比特密文数据。

14. 在使用RSA的公钥体制中，已截获发给某用户的密文为c=10，该用户的公钥pk=5，n=35，那么明文m应该为多少？

答：需要求出解密密钥d。

已知N =35，则只有一种可能，即p*q=5*7=35；(p-1)*(q-1)=4*6=24。

根据公式 $d \times e \equiv 1 \pmod{(p-1)(q-1)}$，又e=5，所以

$5*d \equiv 1 \pmod{24}$，即 $5*d \bmod 24 = 1$。

由此推测5*5=25。即25除以24刚好余1。所以d=5。

密文 $c = m^e \bmod N = m^5 \bmod 35 = 10$。

明文 $m = c^d \bmod N = 10^5 \bmod 35 = 5$。

15. 利用RSA算法运算，如果p=11，q=13，pk=103，对明文3进行加密。求sk及密文。

答：N = p*q=11*13=143；(p-1)*(q-1)=10*12=120

根据公式 $d \times e \equiv 1 \pmod{(p-1)(q-1)}$ 又e=103，所以

$103*d \equiv 1 \pmod{120}$。即 $103*d \bmod 120 = 1$。

103x7=721。721除以120刚好余1。所以d=7。

密文 $c = m^e \bmod N = 3^{103} \bmod 143 = 16$。

16. 在RSA体制中，假设某用户的公钥是3533，p=101，q=113，请对明文9726加密和解密。

答：N = p*q=101*113= 1,1413；(p-1)*(q-1)=100*112=11200。

密文 $c = m^e \bmod N = 9726^{3533} \bmod 11413$。因为数据太大，可能会存在溢出。

17. 简述位置k-匿名的思想，说明其在位置隐私保护中的作用。

答：当一个移动用户的位置无法与其他 k-1个用户的位置相区别时，称此位置满足位置 k-匿名。

18. 简述基于赫尔伯特曲线的空间数据加密原理。

答：其核心思想是：将空间中的用户位置及查询点位置单向转换到一个加密空间，在加密空间中进行查询。该方法首先将整个空间旋转一个角度，在旋转后的空间中建立Hilbert曲线。用户提出查询时，根据Hilbert曲线将自己的位置转换成Hilbert值，提交给服务提供者；服务提供者从被查询点中找出Hilbert值与用户Hilbert值最近的点，并将其返回给用户。

第8章 物联网典型应用

1.简述物联网在环境监控中的应用架构。

答：环境物联网的基本系统架构分为感知层、传输层和应用层，其作用可形象表述为传感、传送、传导和传达（即四传）。感知层对应了测量、感知环境污染监控因子的仪器仪表、现场传感器等（即传感），网络层对应各种可用的有线和无线网络（即传送），应用层则对应环境自动监控的具体业务逻辑的实现

2.简述物联网在智能交通中的应用架构。

答：智能交通管理系统（ITMS）是通过先进的交通信息采集技术、数据通信传输技术、电子控制技术和计算机处理技术等，把采集到的各种道路交通信息和各种交通服务信息传输到交通控制中心，交通控制中心对交通信息采集系统所获得的实时交通信息进行分析、处理，并利用交通控制管理优化模型进行交通控制策略、交通组织管理措施的优化。交通信息分析、处理和优化后的交通控制方案和交通服务信息等内容通过数据通信传输设备分别传输给各种交通控制设备和交通系统的各类用户，以实现对道路交通的优化控制，为各类用户提供全面的交通信息服务。

3.简述物联网在智能家居中的应用架构。

答：基于物联网的智能家居，表现为利用信息传感设备（同居住环境中的各种物品松耦合或紧耦合）将与家居生活有关的各种子系统有机地结合在一起，并与互联网连接起来，进行监控、管理信息交换和通信，实现家居智能化，包括：智能家居（中央）控制管理系统、终端（家居传感器终端、控制器）、家庭网络、外联网络、信息中心等。

4.简述物联网应用中需要解决的关键技术。

答：传感器选择，传输方式选择，数据存储模式选择，数据分析算法选择，安全保障技术选择等。

5.试提出物联网在环境控制、智能家居以及交通管理中一种新的应用实例。

答：略

6.简述物联网在工业流程管理中的作用和意义。

答：物联网在工业领域的应用主要集中在以下几个方面：制造业供应链管理、生产过程工艺优化、产品设备监控管理、环保监测及能源管理、工业安全生产管

理。

7. 设想基于物联网的未来养老模式，并给出一种应用方案。

答：设计一种智康监护系统，其基于物联网的智慧养老解决方案主要由四个方面组成。分别为数据采集子系统、紧急呼叫子系统、信息交互子系统、适老化基础设施。