# RFID 复习天线的作用是

1. 填空题

1、自动识别技术是应用一定的识别装置，通过被识别物品和识别装置之间的接近活动，自动地获取被识别物品的相关信息，常见的自动识别技术有**语音识别技术**、**图像识别技术**、**射频识别技术**、**条码识别技术**（至少列出四种）。

2、RFID的英文缩写是**Radio Frequency IDentification**。

3、RFID系统通常由**电子标签**、**读写器**和**上层管理软件**三部分组成。

4、在RFID系统工作的信道中存在有三种事件模型：

①**以能量提供为基础的事件模型**

②**以时序方式提供数据交换的事件模型**

③**以数据交换为目的的事件模型**

5、时序指的是读写器和电子标签的工作次序。通常，电子标签有两种时序：

一种是 **读写器先发言**(RTF（Reader Talk First）) ；

另一种是 **标签先发言**(TTF（Target Talk First）) 。

6、读写器和电子标签通过各自的天线构建了二者之间的非接触信息传输通道。根据观测点与天线之间的距离由近及远可以将天线周围的场划分为三个区域：**非辐射场区**、**辐射近场区**、**辐射远场区**。

7、上一题中第二个场区与第三个场区的分界距离R为**R=2D2/λ**。（已知天线直径为D，天线波长为。）

8、在RFID系统中，读写器与电子标签之间能量与数据的传递都是利用耦合元件实现的，RFID系统中的耦合方式有两种：**电感耦合式**、**电磁反向散射耦合式**。

9、读写器和电子标签之间的数据交换方式也可以划分为两种，分别是**负载调制**、**反向散射调制**。

10、按照射频识别系统的基本工作方式来划分，可以将射频识别系统分为**全双工**、**半双工**、**时序系统**。

11、读写器天线发射的电磁波是以球面波的形式向外空间传播，所以距离读写器R处的电子标签的功率密度S为（读写器的发射功率为PTx，读写器发射天线的增益为GTx，电子标签与读写器之间的距离为R）：**S= （PTx·GTx）/（4πR2）**。

12、按照读写器和电子标签之间的作用距离可以将射频识别系统划分为三类：

**密耦合系统{典型作用距离为0~1cm}**、**遥耦合系统（近耦合系统{典型作用距离为15cm}和疏耦合系统{典型作用距离为1m}）**、**远距离系统{典型作用距离为1~10m}**。

前面三种系统各有自己适合的读写器(CCD\PCD\VCD)和电子标签(CICC\PICC\VICC)。

14443标准对应近耦合系统，15693标准对应疏耦合系统。

13、典型的读写器终端一般由**天线**、**射频模块**、**逻辑控制模块**三部分构成。

14、控制系统和应用软件之间的数据交换主要通过读写器的接口来完成。一般读写器的I/O接口形式主要有：**USB**、**WLAN**、**以太网接口**、**RS-232串行接口**、**RS-485串行接口**。

15、随着RFID技术的不断发展，越来越多的应用对RFID系统的读写器也提出了更高的要求，未来的读写器也将朝着**多功能**、**小型化**、**便携式**、**嵌入式**、**模块化**的方向发展。

16、从功能上来说，电子标签一般由**天线**、**调制器**、**编码发生器**、**时钟**、**存储电路**组成。

17、读写器之所以非常重要，这是由它的功能所决定的，它的主要功能有：

**与电子标签通信**、**标签供能**、**多标签识别**、**移动目标识别**。

18、根据电子标签工作时所需的能量来源，可以将电子标签分为**有源/无源标签**。

19、按照不同的封装材质，可以将电子标签分为**纸**、**塑料**、**玻璃**。

20、电子标签的技术参数主要有**传输速率**、**读写速度**、**工作频率**、**能量需求**。

21、未来的电子标签将有以下的发展趋势：**成本低**，**体积小**，**容量大**，**工作距离远**。

22、完整性是指信息未经授权不能进行改变的特性，保证信息完整性的主要方法包括以下几种：

**协议**、**纠错编码方法**、**密码校验和方法**、**数字签名**、**公证**。

23、常用的差错控制方式主要有**检错重发**、**前向纠错**、**混合纠错**。

24、差错控制时所使用的编码，常称为纠错编码。根据码的用途，可分为**检错码**和**纠错码**。

25、在发送端需要在信息码元序列中增加一些差错控制码元，它们称为**监督码元**。

26、设信息位的个数为k，监督位的个数为r，码长为n=k+r，则汉明不等式为：**2r-1≥n**。

27、两个码组中对应位上数字不同的位数称为**码距**，又称**汉明距离**，用符号D（a，b）表示，如两个二元序列a=111001，b=101101，则D（a，b）=**2**。

28、最常用的差错控制编码方法有**奇偶校验**、**循环冗余校验**、**汉明码（也称海明码）**。

29、在偶校验法中，无论信息位多少，监督位只有1位，它使码组中“1”的数目为**偶数**。

30、常用的奇偶检验法为**垂直奇偶校验**、**水平奇偶校验**、**垂直水平奇偶校验**。

31、RFID系统中的数据传输也分为两种方式：阅读器向电子标签的数据传输，称为**下行链路传输**；电子标签向阅读器的数据传输，称为**上行链路传输**。

32、电感耦合式系统的工作模型类似于变压器模型。其中变压器的初级和次级线圈分别是：

**阅读器天线线圈**和**电子标签天线线圈**。

33、电子标签按照天线的类型不同可以划分为**线圈型**、**微带贴片型**、**偶极子型**三种。

34、随着RFID技术的进一步推广，一些问题也相应出现，这些问题制约着它的发展，其中最为显著的是数据安全问题。数据安全主要解决**数据保密**和**认证**的问题。

35、常见的密码算法体制有**对称密码体系**和**非对称密码体系**两种。

36、根据是否破坏智能卡芯片的物理封装，可以将智能卡的攻击技术分为**破坏性攻击**、**非破坏性攻击**。

37、RFID系统中有两种类型的通信碰撞存在，一种是**阅读器碰撞**，另一种是**电子标签碰撞**。

38、为了防止碰撞的发生，射频识别系统中需要设计相应的防碰撞技术，在通信中这种技术也称为多址技术，多址技术主要分为以下四种：**空/频/码/时分多址**。

39、TDMA算法又可以分为**基于概率的ALOHA算法**和**确定的二进制树型算法**两种。

40、上述两种TDMA算法中，会出现“饿死”现象的算法是**基于概率的ALOHA算法**。

41、基于概率的ALOHA算法又可以分为：

**纯ALOHA算法**、**时隙ALOHA算法**、**帧时隙ALOHA算法**、**动态帧时隙ALOHA算法**等。

42、物联网(Internet of things)被称为是信息技术的一次革命性创新，成为国内外IT业界和社会关注

的焦点之一。它可以分为**标识**、**感知**、**处理**、**信息传送**四个环节。

43、上述物联网四个环节对应的关键技术分别为**RFID**、**传感器**、**智能芯片**、**无线传输网络**。

44、RFID系统按照工作频率分类，可以分为**低频**、**高频**、**超高频**、**微波**四类。（频率分段P61）

45、高频RFID系统典型的工作频率是**13.56MHz**。

46、超高频RFID系统遵循的通信协议一般是**ISO18000-7**、**ISO18000-6**。

47、目前国际上与RFID相关的通信标准主要有：**ISO/IEC 18000标准**、**EPC Global 标准**。

48、电子标签含有物品唯一标识体系的编码，其中**电子产品代码（EPC）**是全球产品代码的一个分支，它包含著一系列的数据和信息，如产地、日期代码和其他关键的供应信息。

49、超高频RFID系统的识别距离一般为**1~10m**。

50、超高频RFID系统数据传输速率高，可达**1kb/s**。

51、RFID系统的天线生产工艺主要有 **线圈绕制法 、蚀刻法 、印刷法** 。

52、在通信系统中，比特率是指 **每秒钟通过信道传输的信息量** 。

53、在谐振电路中，常用品质因数描述电路的 **能耗** 。

54、低频段、高频段RFID读写器的射频前端采用 **串联** 谐振电路，而电子标签的射频前端采用 **并联** 谐振电路。

55、低、高频RFID系统中标签向读写器传送数据的调制技术主要有 **电阻负载调制** 和  
 **电容负载调制** 。

56、在无线通信中，天线的作用是 **发射和接收无线电波**

57、电阻负载调制是通过 **数据流** 控制电子标签 **负载阻抗大小** 来向读写器传输数据的方法。

58、在RFID系统中，实现数据完整性的措施是**差错控制**和**防碰撞算法**。

59、在RFID系统中，实现数据安全的措施是**数据加密**和**认证技术**。

60、RFID系统的工作频率一般选择在 **ISM**  频段（ISM: Industrial Scientific Medical Band,即此频段主要是开放给工业、科学、医学三个主要机构使用）。

61、在射频系统中，振荡器的作用是 **将直流功率转换为射频功率** 。

62、在通信系统中，波特率是指 **每秒钟通过信道传输的码元数量（数据信号对载波的调制速率）** 。

63、常见的密码算法体制有 **公钥密码 、 分组密码 、 序列密码** 。

64、电子标签含有物品唯一标识体系编码，其中应用最为广泛的一种编码为 **EPC编码（电子产品编码）** 。

65、RFID技术是通过 **射频信号** 获取物体的相关数据，并识别物体的技术。

66、在差错控制中，经常在发送端需要的码元序列中增加一些差错控制码元，这些码元通常称为 **监督码** 。

67、在谐振电路中，电感L与电容C满足 **电感储存的平均能量与电容储存的平均能量相等（输入阻抗为纯电阻）** 时，电路会产生谐振。

68、常见的载波调制方法有 **振幅键控 、 频移键控 、 相移键控** 。

69、RFID系统中有两种类型的通信碰撞存在，一种是**阅读器碰撞**，另一种是**电子标签碰撞**。

70、**传感器作用：**传感器处于研究对象与检测系统的接口位置，是感知、获取与检测信息的窗口，它提供物联网系统赖以进行决策和处理所必需的原始数据。

71、**传感器组成：**传感器一般由敏感元件、转换元件、基本转换电路组成。

72、分辨率是指传感器能够感知或检测到的最小输入信号增量。分辨率可以用绝对值或与满量程的百分比来表示。

73、**传感器的数学模型**

传感器的理想动态特性：当输入量随时间变化时，输出量能立即随之无失真地变化。

实际上：存在弹性、惯性、阻尼元件，与输入量、输入量的变化速度、输入量变化的加速度等有关

工程上常用**线性时不变系统理论**来描述传感器的动态特性

用常系数线性微分方程（**线性定常系统**）表示传感器输出量与输入量的关系

74、**灵敏度**：传感器在稳态信号作用下输出量变化对输入量变化的比值

1. **线性度：**传感器的输入、输出间成线性关系的程度
2. **重复性：**传感器在输入量按同一方向作全量程多次测试时所得输入－输出特性曲线一致的程度

77、**智能传感器**：（intelligent sensor）具有信息处理功能的传感器。智能传感器带有微处理机，具有采集、处理、交换信息的能力，是传感器集成化与微处理机相结合的产物。

二、选择题

1、下列哪一项不是低频RFID系统的特点？（ A ）

A、它遵循的通信协议是ISO18000-3 B、它采用标准CMOS工艺，技术简单

C、它的通信速度低 D、它的识别距离短(<10cm)

2、下列哪一项是超高频RFID系统的工作频率范围？（ B ）

A、<150KHz B、433.92MHz 和860～960MHz C、13.56MHz D、2.45～5.8GHz

3、ISO18000-3、ISO14443和ISO15693这三项通信协议针对的是哪一类RFID系统？（ B ）

A、低频系统 B、高频系统 C、超高频系统 D、微波系统

4、未来RFID的发展趋势是（ C ）。

A低频RFID B、高频RFID C、超高频RFID D、微波RFID

5、中国政府在2007年发布了《关于发布（ D ）频段射频识别(RFID)技术应用试行规定的通知》。

A 、<150KHz B、13.56MHz C、2.45～5.8GHz D、800/900MHz

6、上述通知规定了中国UHF RFID技术的试用频率为（ C ）。

A、125KHz B、13.56MHz C、840-845MHz和920-925 MHz D、433.92MHz

7、下列哪一载波频段的RFID系统拥有最高的带宽和通信速率、最长的识别距离和最小的天线尺寸？（ D ）

A、<150KHz B、433.92MHz 和860～960MHz C、13.56MHz D、2.45～5.8GHz

8、在一个RFID系统中，下列哪一个部件一般占总投资的60%至70%？（ A ）

A、电子标签 B、读写器 C、天线 D、应用软件

9、（ 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。

A、天线 B、电子标签芯片 C、射频接口 D、读写模块

10、绝大多数射频识别系统的耦合方式是（ A ）。

A、电感耦合式 B、电磁反向散射耦合式 C、电容负载耦合式 D、电阻负载耦合式

11、在RFID系统中，电子标签的天线必须满足一些性能要求。下列几项要求中哪一项不需要满足（ D ）。

A、体积要足够小 B、要具有鲁棒性 C、价格不应过高 D、阻抗要足够大

12、读写器中负责将读写器中的电流信号转换成射频信号并发送给电子标签，或者接收标签发送过来的射频信号并将其转化为电流信号的设备是（ B ）。

A、射频模块 B、天线 C、读写模块 D、控制模块

13、任意一个由二进制位串组成的代码都可以和一个系数仅为‘0’和‘1’取值的多项式一一对应。则二进制代码10111对应的多项式为（ A ）。

A、x4+x2+x+1 B、x6+x4+x2+x+1 C、x5+x3+x2+x+1 D、x5+x3+x+1

14、在射频识别系统中，识读率和误码率是用户最为关心的问题。已知待识读标签数为NA，正确识读的标签数为NR，每个标签的码元数为NL，读写器识读出发生错误的码元总数为NE，则识读率为（ C ）。

A、 B、 C、 D、

15、若对下列数字采用垂直奇校验法，则最后一行的监督码元为（ C ）。

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 位/数字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| C1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| C2 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| C3 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| C4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| C5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| C6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| C7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 奇校验 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |

A、0110100110 B、0110111001 C、1001011001 D、1001100001

16、在射频识别应用系统上主要采用三种传输信息保护方式，下列哪一种不是射频识别应用系统采用的传输信息保护方式：（ D ）。

A、认证传输方式 B、加密传输方式 C、混合传输方式 D、分组传输方式

17、电子标签正常工作所需要的能量全部是由阅读器供给的，这一类电子标签称为（ B ）。

A、有源标签 B、无源标签 C、半有源标签 D、半无源标签

18、在天线周围的场区中有一类场区，在该区域里辐射场的角度分布与距天线口径的距离远近是不相关的。这一类场区称为（ A ）。

A、辐射远场区 B、辐射近场区 C、非辐射场区 D、无功近场区

19、在防碰撞算法中，非确定性算法是（ C ）。

A、基于随机数和时隙的二进制树搜索算法 B、动态二进制数型搜索算法

C、动态时隙ALOHA D、二进制树型搜索算法

20、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，则碰撞周期为（ A ）。

A、2T0 B、T0 C、t+T0 D、0.5T0

21、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 ）。

A、 B、 C、 D、

22、RFID信息系统可能受到的威胁有两类：一类是物理环境威胁，一类是人员威胁，下列哪一项属于人员威胁（ D ）。

A、电磁干扰 B、断电 C、设备故障 D、重放攻击

23、RFID系统面临的攻击手段主要有主动攻击和被动攻击两种。下列哪一项属于被动攻击（ C ）。

A、获得RFID标签的实体，通过物理手段进行目标标签的重构。

B、用软件利用微处理器的通用接口，寻求安全协议加密算法及其实现弱点，从而删除或篡改标签内容。

C、采用窃听技术，分析微处理器正常工作过程中产生的各种电磁特征，获得RFID标签和阅读器之间的通信数据。

D、通过干扰广播或其他手段，产生异常的应用环境，使合法处理器产生故障，拒绝服务器攻击等。

24、通信双方都拥有一个相同的保密的密钥来进行加密、解密，即使二者不同，也能够由其中一个很容易的推导出另外一个。该类密码体制称为（ B ）。

A、非对称密码体制 B、对称密码体制 C、RSA算法 D、私人密码体制

25、射频识别系统中的加密数据传输所采用的密码体制是（ D ）。

A、非对称密码体制 B、RSA算法 C、DES算法 D、序列密码体制

26、当读写器发出的命令以及数据信息发生传输错误时，如果被电子标签接收到，那么不会导致以下哪项结果（ A ）。

A、读写器将一个电子标签判别为另一个电子标签，造成识别错误；

B、电子标签错误的响应读写器的命令；

C、电子标签的工作状态发生混乱；

D、电子标签错误的进入休眠状态。

27、设编码序列中信息码元数量为k，总码元数量为n，则比值k/n 就是（ D ）。

A、多余度 B、冗余度 C、监督码元 D、编码效率

28、射频识别系统中的哪一个器件的工作频率决定了整个射频识别系统的工作频率，功率大小决定了整个射频识别系统的工作距离（ C ）。

A、电子标签 B、上位机 C、读写器 D、计算机通信网络

29、工作在13.56MHz频段的RFID系统其识别距离一般为（ C ）。

A、<1cm B、<10cm C、<75cm D、10m

30 、RFID高频的频率范围为：（ B ）

A、30-300KHz B、3-30MHz C、300MHz以上 D、860-960MHz

31、根据射频标签工作方式分为（ A ）、被动式、半被动式三种类型。

A、主动式 B、只读式 C、一次性编程只读式 D、可重复编程只读式

32、射频识别（RFID）是物联网的关键技术之一，RFID标签又称为电子标签，关于电子标签与条型码标签的描述，（ D ）是正确的。

A、电子标签建设成本低，多个标签可被同时读取。

B、条型码标签容量小，但难以被复制。

C、电子标签通讯距离短，但对环境变化有较高的忍受能力。

D、电子标签容量大，可同时读取多个标签并且难以被复制。

33、RFID技术作为一项先进的自动识别和数据采集技术，被公认为21世纪十大重要技术之一，已经成功应用到生产制造、物流管理、公共安全等领域，RFID在发展过程中也遇到了很多问题，下面哪一项不是（ A ）

A、标准的不统一

B、隐私权问题、安全问题

C、成本问题、就业问题

D、自动识别技术不成熟

34、射频识别标准大致包括哪几类（ A ），其中编码标准和通信协议（即通讯接口）是争夺得比较激烈的部分，他们也构成了RFID标准的核心。

①技术标准（如符合、射频识别技术、IC卡标准等）

②数据内容标准（如编码格式、语法标准等）

③一致性标准（如印刷质量、测试规格等标准）

④应用标准（如船运标签、产品包装标签等）

A、①②③④ B、①②④ C、①③④ D、②③④

35、电感耦合系统可以不包括（ B ）

A、密耦合系统、 B、反向散射耦合系统 C、近耦合系统、 D、疏耦合系统

36、在ISO/IEC15693中没有相关的数据元素定义的是（ A ）

A、CID(卡标识符) B、UID（唯一标识符） C、AFI（应用簇标志符） D、DSFID（数据存储格式标识符）

37、下列哪种不属于RFID三种工作模型中的（ A ）

A、以应答方式完成数据传输的工作模型

B、以能量供给为基础的工作模型

C、以时序方式完成数据传输的工作模型

D、以数据传输为目的的工作模型

38、下列哪种不属于RFID差错控制方式是（ B ）

A、前向纠错 B、自动检错 C、混合纠错 D、检错重发

39、下列哪种不属于RFID系统的组成部分是（ C ）。

A、电子标签 B、读写器 C、刷卡器 D、上层管理系统

40、超高频RFID系统遵循的通信协议一般是（ D ）。

A、ISO18000-2 B、ISO18000-3 C、ISO18000-5 D、ISO18000-7

41、以下不属于ISM频段的工作频率是（ A ）

A、低频（LF） B、高频(HF) C、超高频(UHF) D、微波(µW)

42、电感耦合电子标签与读写器之间的工作距离（ A ）

A、<1m B、>1m C、<1cm D、>1cm

43、电感耦合方式的电子标签多为（ A ）

A、无源 B、半无源 C、有源 D、不确定

44、RFID电子标签常见存储器中只能读的是（ D ）

A、EEPROM B、SRAM C、FRAM D、ROM

45、常用于远距离RFID系统的天线是（ A ）

A、微带贴片天线 B、偶极子天线 C、线圈天线 D、其他天线

46、第二代身份证是符合（ B ）协议的射频卡

A、ISO/IEC14443 TYPE A B、ISO/IEC14443 TYPE B

C、ISO/IEC 15693 D、ISO/IEC 18000-C

47、脉冲调制是指将数据的NRZ码变换为（ C ）频率的脉冲串

A、更低 B、相等 C、更高 D、不确定

48、任意一个由二进制位串组成的代码都可以和一个系数仅为‘0’和‘1’取值的多项式一一对应。则二进制代码1010111对应的多项式为（ B ）。

A、x4+x2+x+1 B、x6+x4+x2+x+1 C、x5+x3+x2+x+1 D、x5+x3+x+1

49、在RFID系统中，副载波的调制方法主要应用于（C）

A、125kHz从电子标签向读写器的数据传输过程

B、125kHz从读写器向电子标签的数据传输过程

C、13.5MHz从电子标签向读写器的数据传输过程

D、13.5MHz从读写器向电子标签的数据传输过程

50、电子标签正常工作所需要的能量全部是由电池供给的，这一类电子标签称为（ A ）。

A、有源标签 B、无源标签 C、半有源标签 D、半无源标签

51、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3ms，则碰撞周期为（ C ）。

A、8ms B、7ms C、6ms D、5ms

52、在差错控制中，设计思想是对出现的错误尽量纠正，纠正不了则要通过重发来消除错误的差错控制是（ C ）

A、检错重发 B、前向纠错 C、混合纠错 D、都不是

53、若对下列数字采用垂直偶校验法，则最后一行的监督码元为（ B ）。

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 位/数字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| C1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| C2 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| C3 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 |
| C4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| C5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| C6 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| C7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 偶校验 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |

A、0110100110 B、0010110101 C、1001011001 D、1001100001

54、奇偶校验码和循环冗余码都是（ B ）

A、非线性码 B、线性码 C、比特交织码 D、字节交织码

55、在基本二进制算法中，为了从128个标签中找出唯一一个标签，需要进行多次请求，其平均次数为（ B ）。

A、9 B、8 C、7 D、6

56、在RFID系统中，一般采用（D）法来解决碰撞

A、空分多址（SDMA） B、频分多址（FMDA）

C、码分多址（CDMA） D、时分多址（TDMA）

57、在RFID系统防碰撞算法中（ D ）是读写器先发言控制的

A、纯ALOHA B、时隙ALOHA C、动态时隙ALOHA D、二进制树型搜索算法

58、设编码序列中信息码元数量为80，总码元数量为200，则编码效率是（ C ）。

A、80% B、60% C、40% D、20%

59 、RFID超高频的频率范围为：（ D ）

A、30-300KHz B、3-30MHz C、2.45GHz D、860-960MHz

60、攻击分为被动攻击和主动攻击，其中关于被动攻击正确的是（ A ）

A、更改伪造信息 B、拒绝使用资源 C、应对措施是认证技术 D、截获信息

61、根据射频标签工作方式分为主动式、（ A ）、半被动式三种类型。

A、被动式 B、从机式 C、主机式 D、单机式

62、对称密码体制也称（ C ）

A、单钥公钥密码体制 B、双钥公钥密码体制

C、单钥私钥密码体制 D、双钥私钥密码体制

63、下列不属于RFID差错控制方式是（ A ）

A、动态检错 B、前向纠错 C、检错重发 D、混合纠错

64、下列不属于RFID系统的组成部分是（ A ）。

A、数据库服务器 B、电子标签 C、读写器 D、上层管理系统

65、微波RFID系统遵循的通信协议一般是（ C ）。

A、ISO18000-2 B、ISO18000-3 C、ISO18000-5 D、ISO18000-7

66、下列不属于RFID三种工作模型中的（ B ）

A、以能量供给为基础的工作模型

B、以同步方式完成数据传输的工作模型

C、以时序方式完成数据传输的工作模型

D、以数据传输为目的的工作模型

67、工作在2.45GHz频段的RFID系统其识别距离一般为（ D ）。

A、<10cm B、<0.5m C、<1m D、3~5m

68、ISO18000-6、ISO18000-7和ISO/IEC 18047—6这三项通信协议针对的是哪一类RFID系统？（ C ）

A、低频系统 B、高频系统 C、超高频系统 D、微波系统

69、电磁反向散射耦合电子标签与读写器之间的工作距离（ B ）

A、<1m B、>1m C、<1cm D、>1cm

70、电子标签芯片的射频前端包含是（ D ）

A、编/解码电路

B、微处理器

C、EEPROM

D、公共电路

71、ISO/IEC14443标准是（ A ）

A、技术标准 B、数据内容标准 C、性能标准 D、应用标准

72、ISO/IEC14443和ISO/IEC15693的作用距离不同的原因（ B ）

A、工作频率不同 B、载波功率不同 C、工作原理不同 D、工作方式（有源无源）不同

73、ISO/IEC14443标准分TYPEA和TYPE B 两种方式的原因是（ C ）

A、工作频率不同 B、工作原理不同 C、信息传输（编码调制）方式不同 D、工作方式

74、三种耦合卡类型作用距离的关系是（ A ）

A、CICC<PICC<VICC B、CICC<VICC<PICC

C、CICC>PICC>VICC D、CICC>PICC>VICC

75、ISO/IEC18000标准中主要是定义了不同频率下的空中接口参数其中18000-2、18000-3、18000-4、18000-6、18000-7对应的频率是（ A ）

A、< 135kHZ,13.56MHz,2.45GHz,860~930MHz, 433MHz

B、< 135kHZ,13.56MHz, 433MHz ，860~930MHz, 2.45GHz,

C、 2.45GHz,860~930MHz, 433MHz ，13.56MHz, < 135kHZ,

D、433MHz,13.56MHz,2.45GHz,860~930MHz, < 135kHZ

76、在ISO/IEC14443标准中用数据曼彻斯特编码的副载波调制（ASK）信号进行负载调制的信号接口是（ B ）

A、TYPE A 型PCD向PICC通信 B、TYPE A 型PICC向PCD通信  
C、TYPE B 型PCD向PICC通信 D、TYPE B 型PICC向PCD通信

77、电磁反向散射耦合系统典型的工作频率是（ A ）

A、433MHz B、125KHz C、13.56MHz D、225KHz

78、电感耦合系统典型的工作频率是（ C ）

A、433MHz B、915MHz C、13.56MHz D、2.45GHz

79、高频下工作的电子标签采用（ A ）天线。

A、线圈型 B、微带贴片型 C、偶极子型 D、ABC都不是

80、RFID系统的数据传输中，能量供应间歇的系统是（ C ）

A、全双工系统

B、半双工系统

C、时序系统

D、ABC都不是

81、在射频识别系统中，最常用的防碰撞算法是 (C) 。

A、空分多址法 B、频分多址法 C、时分多址法 D、码分多址法。

82、工作在125kHz频段的RFID系统其识别距离一般为 B 。

A、<1cm B、<10cm C、<75cm D、10m

83、 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。

A、天线 B、电子标签芯片 C、射频接口 D、读写模块

84、绝大多数射频识别系统的耦合方式是 A 。

A、电感耦合式 B、电磁反向散射耦合式 C、负载耦合式 D、反向散射调制式

85、在RFID系统中，电子标签的天线必须满足一些性能要求。下列几项要求中哪一项不需要满足 D 。

A、体积要足够小B、要具有鲁棒性 C、价格不应过高 D、阻抗要足够大

86、在电子标签中负责将读写器中的发来射频信号转换为电流信号，或者将自身的电流信号转化为射频信号的设备是 B 。

A、射频模块 B、天线 C、读写模块 D、控制模块

87、在天线周围的场区中有一类场区，在该区域里辐射场的角度分布与距天线口径的距离远近是不相关的。这一类场区称为 A 。

A、辐射远场区 B、辐射近场区 C、非辐射场区 D、无功近场区

88、在射频识别系统中，最常用的防碰撞算法是 C 。

A、空分多址法 B、频分多址法 C、时分多址法 D、码分多址法。

89、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 。

A、 B、 C、 D、

90、RFID信息系统可能受到的威胁有两类：一类是物理环境威胁，一类是人员威胁，下列哪一项属于人员威胁： D 。

A、电磁干扰 B、断电 C、设备故障 D、重放攻击

91、RFID系统面临的攻击手段主要有主动攻击和被动攻击两种。下列哪一项属于被动攻击： C 。

A、获得RFID标签的实体，通过物理手段进行目标标签的重构。

B、用软件利用微处理器的通用接口，寻求安全协议加密算法及其实现弱点，从而删除或篡改标签内容。

C、采用窃听技术，分析微处理器正常工作过程中产生的各种电磁特征，获得RFID标签和阅读器之间的通信数据。

D、通过干扰广播或其他手段，产生异常的应用环境，使合法处理器产生故障，拒绝服务器攻击等。

92、通信双方都拥有一个相同的保密的密钥来进行加密、解密，即使二者不同，也能够由其中一个很容易的推导出另外一个。该类密码体制称为 B 。

A、非对称密码体制 B、对称密码体制 C、RSA算法 D、私人密码体制

93、射频识别系统中的加密数据传输所采用的密码体制是 D 。

A、非对称密码体制 B、RSA算法 C、DES算法 D、序列密码体制

94、当读写器发出的命令以及数据信息发生传输错误时，如果被电子标签接收到，那么不会导致以下哪项结果： A 。

A、读写器将一个电子标签判别为另一个电子标签，造成识别错误；

B、电子标签错误的响应读写器的命令；

C、电子标签的工作状态发生混乱；

D、电子标签错误的进入休眠状态。

95、设编码序列中信息码元数量为k，总码元数量为n，则比值k/n 就是 D 。

A、多余度 B、冗余度 C、监督码元 D、编码效率

96、射频识别系统中的哪一个器件的工作频率决定了整个射频识别系统的工作频率，功率大小决定了整个射频识别系统的工作距离： C 。

A、电子标签 B、上位机 C、读写器 D、计算机通信网络

97、分辨率是指传感器能够感知或检测到的最小输入信号增量。分辨率可以用下列哪种来表示。（ D ）

A、绝对值 B、百分比

C、都不可以 D、都可以

98、工程上常用下列哪种理论来描述传感器的动态特性（ A ）。

A、线性时不变系统理论 B、非线性时不变系统理论

C、线性时变系统理论 D、非线性时变系统理论

99、传感器在稳态信号作用下输出量变化对输入量变化的比值反应下列哪种性能（ A ）

A、灵敏度 B、分辨率

C、重复性 D、线性度

100、智能传感器具有哪种性能（ D ）

A、采集 B、处理

C、交换 D、都有

1、 A 2、B 3、B 4、C 5、D 6、C 7、D 8、A 9、B 10、A

11、D 12、B 13、A 14、C 15、C 16、D 17、B 18、A 19、C 20、A

21、B 22、D 23、C 24、B 25、D 26、A 27、D 28、C 29、C 30、B

31、A 32、D 33、A 34、A 35、B 36、A 37、A 38、B 39、C 40、D

41、 A 42、A 43、A 44、D 45、A 46、B 47、C 48、B 49、C 50、A

51、C 52、C 53、B 54、B 55、B 56、D 57、D 58、C 59、D 60、A

61、A 62、C 63、A 64、A 65、C 66、B 67、D 68、C 69、B 70、D

71、A 72、B 73、C 74、A 75、A 76、B 77、A 78、C 79、A 80、C

81、C 82、B 83、B 84、A 85、D 86、B 87、A 88、C 89、B 90、D

91、C 92、B 93、D 94、A 95、D 96、C 97、D 98、A 99、A 100、D

理论部分：

第一部分 物联网概论

1. 物联网Internet of things

分为**标识、感知、处理和信息传送**四个环节，对应的关键技术为**RFID、传感器、智能芯片和无线传输网络**。

中国——感知中国

美国“智能电网”和“智慧地球”

欧洲“物联网行动计划”

日韩“U-Japan”和“U-Korea”战略

新加坡“智慧国2015”发展蓝图

EPC系统组成结构

第二部分 RFID系统概论

**一、RFID——Radio Frequency Identification**

RFID利用射频信号通过**空间耦合**实现无接触信息传递达到识别目标的技术。系统通常**读写器**、**电子标签**及**应用软件**组成。可用于物流，电子票证，动物或资产追踪管理，供应冷链，高速公路智能收费等领域。

**（无线传输频段划分见P61）**

**二、工作原理：**读写器控制射频模块发出射频信号，电子标签主动发送（有源标签）或者凭借感应电流所获得的能量（无源标签）发送出芯片中的存储信息，接收标签的应答，读写器对标签的传递过来的信息进行解码，并传输到主机进行数据处理。

1）在**低频段**(100MHz以下)基于**电感耦合（近距）**

2）在**高频段**(400MHz以上)基于**电磁反向散射耦合（雷达，远距）**

**三、按工作频段分类：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 频段 | 工作频段 | 通信标准协议 | 优点 | 缺点 |
| 低频（LF）30-300KHz | 低频（LF）  <125KHz | ISO18000-2  ISO11785 | 标准CMOS工艺  技术简单可靠成熟  无频率限制 | 通信速度低  识别距离短(<10cm)  天线尺寸大 |
| 高频（HF）3-30MHz | 高频（HF）  13.56MHz | ISO18000-3  ISO14443  ISO15693 | 与标准CMOS工艺兼容  技术可靠成熟  在交通智能卡等领域应用广泛 | 距离不够远(<75cm)  天线尺寸大，  受金属材料等影响大 |
| 超高频（UHF）300-1000MHz | 超高频（UHF）  433MHz、840-845MHz  920-925 MHz | ISO18000-6  ISO18000-7 | 长距离定向识别  天线尺寸小，可绕射，无需可视距离，  发展潜力巨大 | 各国有不同的频段管制，  受金属和液体等材料影响较大  对人体有伤害，限制发射功率 |
| 微波  2.45、5.8GHz | 微波  2.45～5.8GHz | ISO18000-4  DSRC | 除了UHF特性外  更高的带宽和通信速率  更长识别距离，更小的天线尺寸 | ISM频段共享产品多  易受干扰，技术相对复杂  对人体有伤害，限制发射功率 |

第三部分 RFID的工作原理

**一、RFID工作原理**

* 阅读器通过天线向周围空间发送一定频率的射频信号;
* 标签一旦进入阅读器天线的作用区域将产生感应电流，获得能量被激活;激活标签将自身信息编码后经天线发送出去;
* 阅读器接收该信息，经过解码后必要时送至后台网络;
* 后台网络中主机鉴定标签身份的合法性，只对合法标签进行相关处理，通过向前端发送指令信号控制阅读器对标签的读写操作;

**二、RFID的三种工作模型**

1）以**能量供给为基础**的工作模型

**无源**电子标签：当标签进入阅读器的工作范围内以后，标签收到阅读器发送的信号，产生感应电流从而激活内部的电路，内部整流电路将射频能量转化为电能，将该能量存储在标签内部的大电容里，进而为其正常工作提供了所需的能量。

**半有源**电子标签：阅读器发送的射频信号只用来激活标签。

**有源**电子标签：只要标签处于阅读器的工作范围以内，就可以主动向阅读器发送信号。

2）以**时序方式完成数据传输**的工作模型

**阅读器先发言**模式（**RTF**, Reader Talk First）

如果阅读器不主动激活电子标签的话，电子标签不会向阅读器发送信号，通常用于**无源标签**。

**电子标签先发言**模式（**TTF**, Tag Talk First）

就算阅读器不激活标签，标签也会主动向阅读器发送信号

3）以**数据传输为目的**的工作模型

**上行链路传输**

电子标签向阅读器的数据传输。

**下行链路传输**

阅读器向电子标签的数据传输。

离线写入：无论是哪一类电子标签都有离线写入这种情况。所有电子标签在出厂之前都要由生产厂家将标签的ID号（EPC）固化写入，该ID号是标签的身份标识，是唯一的，一旦写入以后将永远不能修改。

在线写入：拓展高级功能，可写标签，结构复杂，成本高。

1. **RFID防碰撞理论**

**1）碰撞的种类**

阅读器碰撞：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。

电子标签碰撞：多个标签同时响应阅读器的命令而发送信息，使阅读器无法识别标签。

**2）传统解决方案**

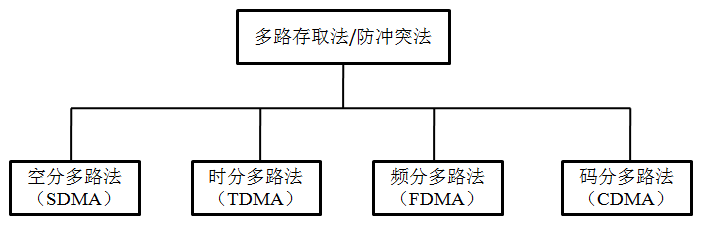
1）空分多址（SDMA）

2）频分多址（FDMA）

3）码分多址（CDMA）

4）时分多址（TDMA）

应用最广泛，又可以分为**基于概率的ALOHA算法（饿死）**和**确定的二进制树型算法**两种。



**3）ALOHA碰撞算法**

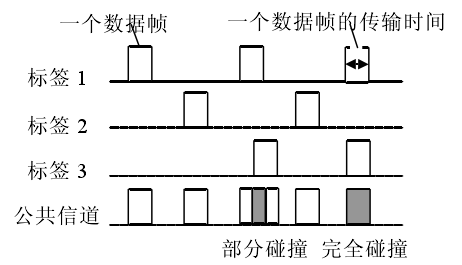
**1、纯ALOHA算法**

（1）主要采用标签先发言（Tag-Talk-First）的方式，即电子标签一旦进入阅读器的工作范围获得能量后，便向阅读器主动发送自身的序列号。

（2）在某个电子标签向阅读器发送数据的过程中，如果有其它电子标签也同时向该阅读器发送数据，此时阅读器接收到的信号就会产生重叠，导致阅读器无法正确识别和读取数据。

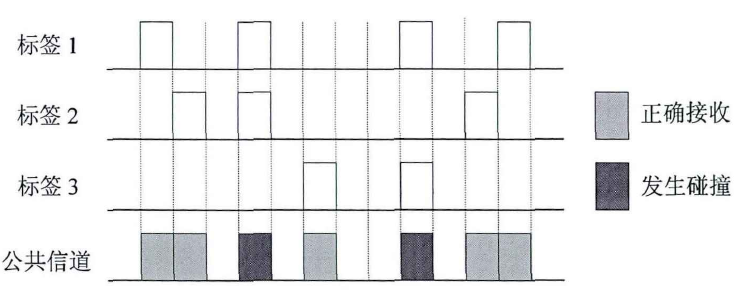
（3）阅读器通过检测并判断接收到的信号是否发生碰撞，一旦发生碰撞，阅读器则向标签发送指令使电子标签停止数据的传送，电子标签接到阅读器的指令后，便随机的延迟一段时间再重新发送数据。

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To，则碰撞时间为2T0。G为数据包交换量，S为吞吐率。



**2、Slotted ALOHA算法：**

* 为提高RFID系统的吞吐率，可以把时间划分为多段等长的时隙，时隙的长度由系统时钟确定，并且规定电子标签只能在每个时隙的开始时才能向阅读器发送数据帧，这就是Slotted ALOHA算法；
* 根据上述规定可得，数据帧要么成功发送，要么完全碰撞，避免了纯ALOHA算法中部分碰撞的发生，使碰撞周期变为To；
* 它是纯ALOHA算法的简单改进，也属于时分多址法，它的缺点是需要同步时钟的控制；



**3、Frame Slotted ALOHA算法（FSA）：**

（1）ALOHA 的另一种改进算法是帧时隙 ALOHA 算法（FSA）。

（2）它是在Slotted ALOHA 算法的基础上把 N 个相同的时隙组成一帧，且在整个电子标签识别过程中，帧的大小是固定的，帧中的每个时隙足够一个电子标签与阅读器进行完通信，该算法也称为固定帧时隙 ALOHA 算法。

（3）该算法比较适用于传输信息量较大的场合，和Slotted ALOHA 算法一样，帧时隙 ALOHA 算法同样需要一个同步开销。

**步骤**

* 首先由阅读器把帧长度 N 发送给电子标签，电子标签则产生[1，N]之间的随机数，接下来各电子标签选择相应的时隙，与阅读器进行通信；
* 如果当前时隙与电子标签随机产生的数相同，电子标签则响应阅读器的命令，若不同，标签则继续等待。
* 假如当前时隙内仅有一个电子标签响应，阅读器就读取该标签发送的数据，读取完了以后就使该标签处于“无声”状态。
* 如果当前时隙内有多个标签响应，则该时隙内的数据就出现了碰撞，此时阅读器会通知该时隙内的标签，让它们在下一轮帧循环中重新产生随机数参与通信。
* 逐帧循环，直到识别出所有电子标签为止。

**4、Dynamic FSA 算法：**

* 该算法根据上一读写周期中统计的成功识别的时隙数、发生碰撞的时隙数、空闲时隙数信息来调整下一读写周期的帧长度。具体调整方法有两种。
* 第一种：根据统计信息，当碰撞时隙数达到规定的上限时，读写器增大下一帧的长度；当碰撞时隙数少于规定的下限时，读写器减少下一帧时隙数。使用该方法当标签规模不大时，读写器使用较短的帧长度就能快速识别标签，而当标签数量很多时，读写器不得不增加帧长度以减少碰撞次数。
* 第二种： 读写器以 2 或 4 个时隙数为一帧开始，如果没有一个标签能够成功识别，读写器增加帧长度开始下一轮读写周期。重复上述过程直到至少有一个标签被成功识别。当有一个标签成功识别后，读写器立刻停止当前的读写周期，然后读写器再以开始时最小的帧长度开始下一轮读写识别。
* 该算法通过动态调整帧长度，相比帧时隙算法在标签规模不大时能够取得较理想的吞吐率。可是一旦标签个数很大时，增大帧长度就不是很好的解决方法，因为帧长度不能无限制的增大。
* 采用ALOHA系列算法，假设阅读器射频工作范围内存在 n 个标签，理论上阅读器至少需要 n 个时隙的时间才能成功识别完，最坏的情况下，阅读器经过多次搜索也未能识别出某个标签，导致出现“饿死现象”。

4）Binary-Tree系列算法

Binary-Tree系列算法（即二进制树型系列搜索算法）由读写器控制，并不会采取退避原则，而是直接进行解决。当多标签同时发送信息而碰撞时，读写器利用碰撞位将碰撞的标签分为两个或更多子集，对每个子集分别识别。如果存在碰撞则继续再划分，直到标签被完全识别为止。这样则有效地避免了标签的“饿死现象”。

该算法有：

（1）二进制树型搜索算法

（2）动态二进制树型搜索算法

（3）基于随机数和时隙的二进制树搜索

举例：

读写器作用范围内有六个电子标签。这六个电子标签的序列号（8位）分别为：

电子标签1: ~~10110010~~

电子标签2: ~~10101011~~

电子标签3: ~~10110011~~

电子标签4: ~~11101011~~

电子标签5: ~~10101010~~

电子标签6: 10100010

二进制树型搜索算法在重复操作的第一次中由读写器发送REQUEST（序列号=11111111）命令。处于读写器作用范围内的标签在同一时刻传输它们的序列号至读写器。每次读写器对收到的标签进行响应。

第一次读写器对收到的标签进行响应11111111，响应结果： 1x1xx01x 。

第二次读写器对收到的标签进行响应10111111，响应结果： 101xx01x 。

第三次读写器对收到的标签进行响应10101111，响应结果： 1010x01x 。

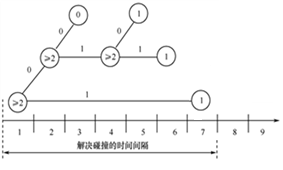
第四次读写器对收到的标签进行响应10100111，响应结果： 10100010 。

第五次读写器对收到的标签进行响应，响应结果： 空 。

若动态二进制树型搜索算法，又是如何进行的。

5）采用随机数和时隙的二进制树形搜索算法，设计一个四层树能解决3张电子标签之间冲突问题的可能结构，在解决这些碰撞的过程中，假设没有新的信息包达到。并简要叙述碰撞解决的过程。

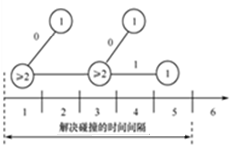
答：设计如下图的四层树能解决3张电子标签之间冲突问题的可能结构：



如上图所示，第一次碰撞在时隙1发生，开始并不知道一共有多少个信息包产生碰撞，每个信息包好像抛硬币一样随机抛得一个0或1，抛0的在时隙2内传输。第二次发生碰撞是在时隙2内，在本例中，两个信息包都是抛1，以致时隙3为空。在时隙4内，时隙2中抛1的两个信息包又一次发生碰撞和分支，抛0的信息包在时隙5内成功传输，抛1的信息包在时隙6内成功传输，所有在时隙1内抛0的信息包之间的碰撞得以解决。在树根时抛1的信息包在时隙7内开始发送信息，没有碰撞发生, 在时隙7内成功传输，这样所有在时隙1内的信息包之间的碰撞得以解决。

6）采用随机数和时隙的二进制树形搜索算法，设计一个三层树能解决3张电子标签之间冲突问题的可能结构，在解决这些碰撞的过程中，假设没有新的信息包达到。并简要叙述碰撞解决的过程。

答：设计如下图的三层树能解决3张电子标签之间冲突问题的可能结构：



如上图所示，第一次碰撞在时隙1发生，开始并不知道一共有多少个信息包产生碰撞，每个信息包好像抛硬币一样随机抛得一个0或1，抛0的在时隙2内成功传输。抛1的信息包在时隙3内开始发送信息，第二次发生碰撞是在时隙3内，再随机抛得一个0或1而分支,抛0的信息包在时隙4内成功传输，抛1的信息包在时隙5内成功传输，所有在时隙1内抛1的信息包也得以解决。这样所有在时隙1内的信息包之间的碰撞得以解决。

5、防碰撞时隙ALOHA算法的原理：

时隙ALOHA算法在ALOHA算法的基础上改进得到。在时隙ALOHA中，帧是由读写器定义的一段时间长度，其中包含若干个时隙。每个标签在每个帧内随机选择一个时隙发送数据。所有标签应答应同步，发送的时隙则随机选择，在发送过程中进行冲突检测，如果存在冲突，则采取退避原则，等待下一个循环周期再发送。按照这种方式，所有的标签完成全部的数据传输给读写器后，重复的过程才会结束。

6、电阻负载调制方式的原理：

在电阻负载调制中，电子标签的负载RL并联一个电阻Rmod, Rmod称为负载调制电阻，该电阻按照数据流的时钟接通和断开，导致标签谐振回路两端的电压发生变化。由于标签和读写器的天线通过耦合方式连接，标签谐振回路端电压的变化导致读写器天线线圈的端电压发生变化，由此产生对读写器电压的调幅。

在调制过程中，首先用数据流信号调制低频率的副载波，该调制副载波用于切换负载电阻，然后采用ASK方式对副载波进行二次调制，最终得到的调制信号被传送到读写器。

7、Mifare S50卡的数据块可分为两种形式, 即普通数据块和数值块。

8、其普通数据块和数值块的区别，以及对数值块类型数据的操作原理及其过程：

普通数据块用于存储一般的16字节数据，仅可以执行READ、WRITE命令。

数值块是特殊的数据块，专门用来存储数值，不仅可以对其执行普通的READ、WRITE命令，还可以执行用于实现电子钱包功能的命令：增值INCREMENT、减值DECREMENT、传送TRANSFER和重存RESTORE。存储在数值块中的数值为四个字节，按特定格式存储。对这种类型的数据的运算，Mifare S50 卡内有专用的运算电路，非常适合公交卡等的应用

数值块中的内容第一次由WRITE命令写入后，以后可用INCREMENT、DECREMENT和RESTORE命令修改其内容，所得结果暂存在其内部的DATA寄存器（数据寄存器）中，然后调用TRANSFER命令即可将结果重新写回数值块。

9、根据下表，当标签RFID尾块数据读出为：“0x 000000000000FF078069FFFFFFFFFFFF”时，说明卡的存储器组织，该扇区对尾块数据的存储控制，并画出Mifare S50卡访问控制条件的存储结构。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 控制位 | | | 访问条件 | | | | | | 说明 |
| 密码A | | 存储控制 | | 密码B | |
| C13 | C23 | C33 | 读 | 写 | 读 | 写 | 读 | 写 | － |
| 0 | 0 | 0 | N | A | A | N | A | A | 密码B可读 |
| 0 | 1 | 0 | N | N | A | N | A | N | 密码B可读 |
| 1 | 0 | 0 | N | B | A/B | N | N | B | － |
| 1 | 1 | 0 | N | N | A/B | N | N | N | － |
| 0 | 0 | 1 | N | A | A | A | A | A | 密码B可读 |
| 0 | 1 | 1 | N | B | A/B | B | N | B | － |
| 1 | 0 | 1 | N | N | A/B | B | N | N | － |
| 1 | 1 | 1 | N | N | A/B | N | N | N | － |

答：Mifare S50卡片的存储容量为8192×1位字长（即1K X 8位字长），采用EEPROM作为存储介质。整个结构划分为16个扇区，编为扇区0～15。每个扇区有4个块（Block）,分别为块0,块1,块2和块3。每个块有16个字节。一个扇区共有 16 Byte X 4 = 64 Byte。扇区0的块0是特殊的块，包含了厂商代码信息，在生产卡片时写入，不可改写。每个扇区的块3（即第四块）也称作尾块， 包含了该扇区的密码A(6个字节)、存取控制(4个字节)、密码B(6个字节)。其余三个块是一般的数据块。

该扇区访问条件在存储结构：

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | | 7 | 8 | 9 | | 10 | 11 | 12 | 13 | 14 | 15 |
|  | 密码A | | | | | | | 存储控制 | | | | 密码B | | | | | | |
|  | 访问控制条件的存储结构 | | | | | | | | | | | | | | | | | |
|  | 位：7 6 5 4 3 2 1 0 | | | | | | | | | | | | | | | | | |
| Byte6 | 3 | | 2 | | 1 | | 0 | | | 3 | | | 2 | | 1 | | 0 | |
| Byte7 | C13 | | C12 | | C11 | | C10 | | | 3 | | | 2 | | 1 | | 0 | |
| Byte8 | C33 | | C32 | | C31 | | C30 | | | C23 | | | C22 | | C21 | | C20 | |
| Byte9 | 0 | | 1 | | 1 | | 0 | | | 1 | | | 0 | | 0 | | 1 | |

注：Byte9是一个备用字节，不对应控制区块的访问条件。

扇区的尾块数据中权限位为：“OxFF078069”， 根据表格，有：

C13=0 C12=0 C11=0 C10=0

C23=0 C22=0 C21=0 C20=0

C33=1 C32=0 C31=0 C30=0

得“C13 C23 C33”=001，在该卡读写权限下可以利用密码A对扇区的尾块可以进行读写操作，可以更改尾块的读写权限，即可以更改密码A、密码B和存储控制位。但不可以利用密码B进行读写操作（此时B密码可读）。

**四、RFID相关电磁场理论**

读写器和电子标签通过各自的天线构建了二者之间的非接触信息传输通道。根据观测点与天线之间的距离由近及远可以将天线周围的场划分为三个区域：

**非辐射场区**：场强与距离天线的远近有关，电磁能量只在场源附近来回流动，随着与天线的距离不断增大，场强不断减小。

分界：R=λ/2π

**辐射近场区**：菲涅尔区，电磁能量会脱离天线的束缚进入到外空间。该区域里辐射场的角度分布与距天线口径的距离远近有关。

分界：R=2D2/λ（已知天线直径为D，天线波长为λ）

**辐射远场区**：夫郎荷费区，该区域里辐射场的角度分布与距天线口径的距离远近是不相关的。

**五、计算题：**

1、设计一个串联谐振电路，要求在RL=25Ω及f=13.56MHZ时，有载品质因数为1.1，求出对应的C、L值，并改变该值使电路在谐振频率不变的情况下品质因数提高为2.2。



解 串联谐振有载品质因数为



所以电感为



谐振时的角频率为

所以电容为

可以通过将电感值提高 倍同时将电容值降低 倍的方法来提高有载品质因数。有载品质提高为原来2倍，即Q=2.2，选 ，电感、电容和有载品质因数分别为





2、设计一个并联谐振电路，要求在RL=50Ω及f=13.56MHZ时，有载品质因数为1.1，求出对应的C、L值，并改变该值使电路在谐振频率不变的情况下品质因数提高为2.2。

解 并联谐振，有载品质因数为

所以电感为

谐振时的角频率为



所以电容为

可以通过将电感值降低 倍同时将电容值提高 倍的方法来提高有载品质因数。要求品质因数为2.2，则选 ，电感、电容和有载品质因数分别为





第四部分 编码与调制

**1.信号工作方式**：

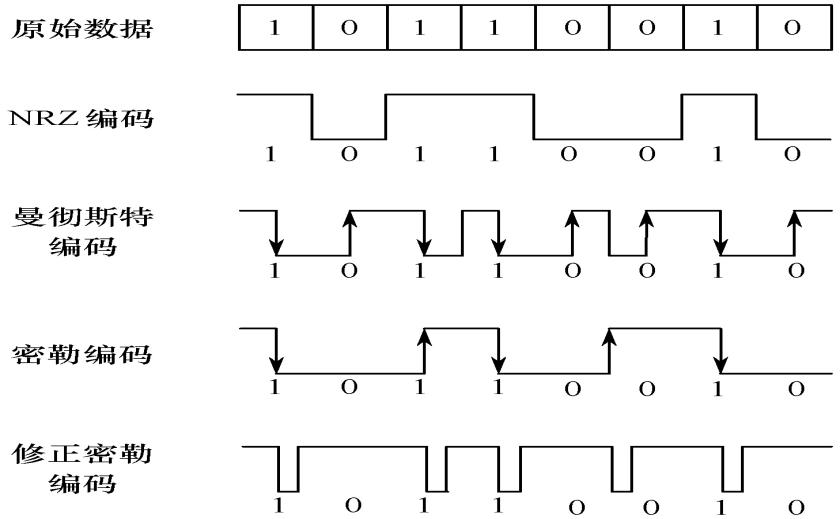
1. 时序系统
2. 全双工系统
3. 半双工系统

2.**信道**

1. 信道带宽
2. 信道传输速率
3. 波特率和比特率
4. 波特率：是指数据信号对载波的调制速率，它用单位时间内载波调制状态改变的次数来表示。
5. 比特率：每秒通过信道传输的信息量称为位传输速率，简称比特率。

（4）信道容量

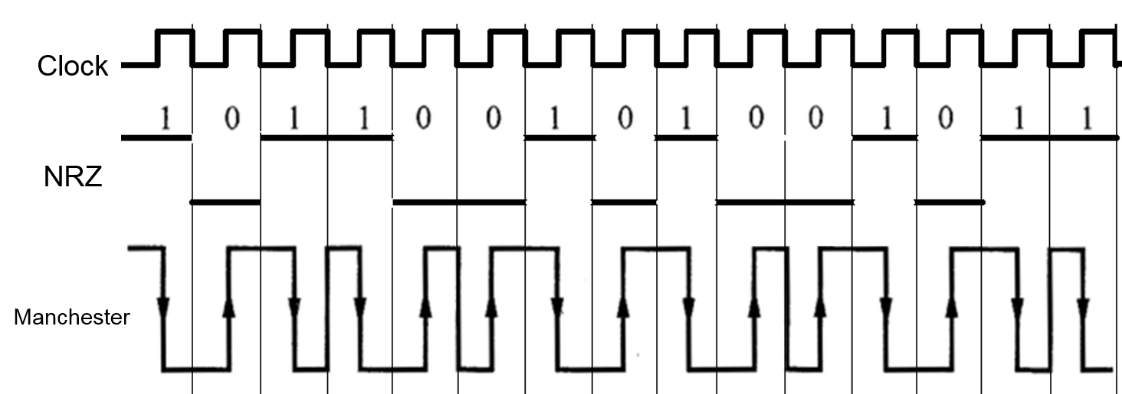
3．典型的编码方式：



**4.曼彻斯特编码**

曼彻斯特编码中用电压的跳变的相位不同来区分0和1，其中从高到低的跳变表示1，从低到高的跳变表示0.

例如：画出数字数据101100101001的曼彻斯特编码。



**5.密勒编码**

密勒编码规则为：对于原始符号“1”，用码元起始不跳变而中心点出现跳变来表示，即用10或01表示；对于原始符号“0”，则分成单个“0”还是连续“0”予以不同的处理，单个“0”时，保持“0”前的电平不变，即在码元边界处电平不跳变，中间点也不跳变；对于连续两个“0”，则使连续两个“0”的边界处发生电平跳变。

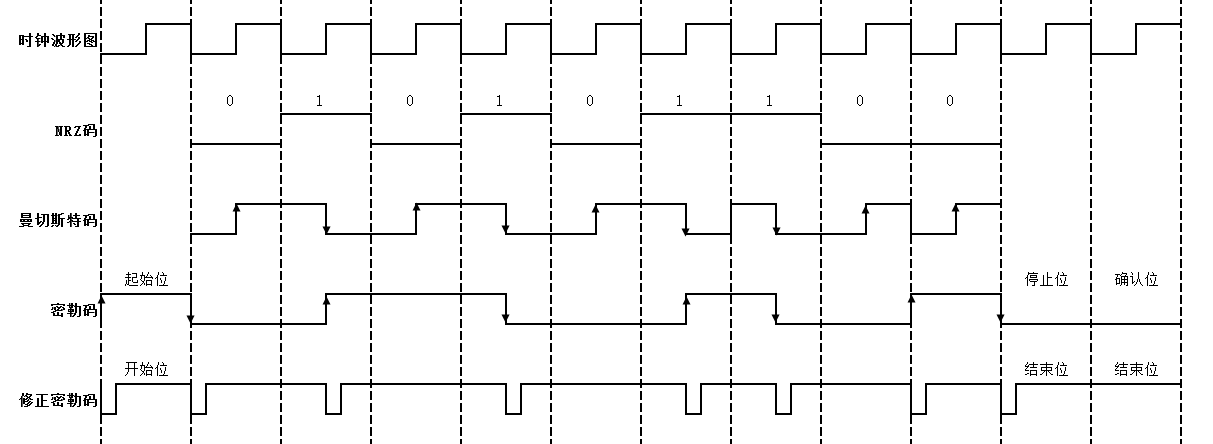
**6.修正密勒编码**

修正密勒编码规则为：每位数据中间有个窄脉冲表示“1”，数据中间没有窄脉冲表示 “0”，对于连续的“0”，则从第二个“0”开始在数据的起始部分增加一个窄脉冲。还有，起始位的开始处有一个窄脉冲，而结束位用“0”表示。如果有两个连续的位开始和中间部分都没有窄脉冲，则表示无信息。

举例：

画出数字信号010101100的时钟图、NRZ编码图、曼彻斯特编码图、密勒码图、修正密勒码图（后两种并画出对应的起始位和停止位）。

提示：参考QQ中作业，注意要求时钟图和相应的编码图周期对应对齐（标准画法）。



注：曼切斯特和密勒码带上箭头。

**7.RFID常用的调制方法**

载波：在信号传输的过程中，并不是将信号直接进行传输，而是将信号与一个固定频率的波进行相互作用，这个过程称为加载，这样一个固定频率的波称为载波。

常用调制方式：

1. 振幅键控
2. 频移键控
3. 相移键控
4. 副载波调制

8、试画出数字信号的几种编码图

第五部分 RFID读写器

**一、读写器的功能**

①**实现与电子标签的通讯**：最常见的就是对标签进行读数，这项功能需要有一个可靠的软件算法确保安全性、可靠性等。除了进行读数以外，有时还需要对标签进行写入，这样就可以对标签批量生产，由用户按照自己需要对标签进行写入；

②**给标签供能**:在标签是被动式或者半被动式的情况下，需要读写器提供能量来激活射频场周围的电子标签；阅读器射频场所能达到的范围主要由天线的大小以及阅读器的输出功率决定的。天线的大小主要是根据应用要求来考虑的，而输出功率在不同国家和地区，都有不同的规定。

③**实现与计算机网络的通讯**

④**实现多标签识别**

⑤**实现移动目标识别**

⑥**实现错误信息提示**

⑦**有源标签的电池信息**

**二、读写器的组成**

****

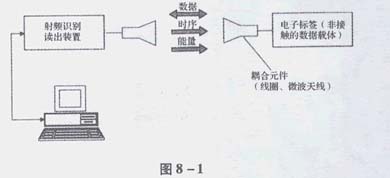
**天线：**

* 发射和接收射频载波信号
* 将读写器中的电流信号转换成射频载波信号并发送给电子标签，或者接收标签发送过来的射频载波信号并将其转化为电流信号；
* 无源标签能量供给

**射频接口模块**

* 包括发射器、射频接收器、时钟发生器和电压调节器等。该模块是读写器的射频前端，负责射频信号的发射及接收。
* 调制电路负责将需要发送给电子标签的信号加以调制，然后再发送；
* 解调电路负责将解调标签送过来的信号并进行放大；
* 时钟发生器负责产生系统的正常工作时钟。

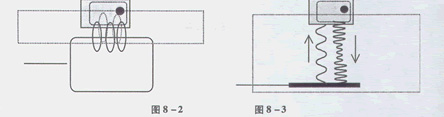
RFID读写器技术原理图:



**逻辑控制模块**

* 读写器的逻辑控制模块是整个读写器工作的控制中心、智能单元，是读写器的“大脑”， 读写器在工作时由逻辑控制模块发出指令，射频接口模块按照不同的指令做出不同的操作。
* 包括微控制器、存储单元和应用接口驱动电路等。
* 微控制器可以完成信号的编解码、数据的加解密以及执行防碰撞算法；
* 存储单元负责存储一些程序和数据；
* 应用接口负责与上位机进行输入或输出的通信。

**读写器的类型：**



电感耦合模型的读写器 电磁反向散射耦合型的RFID读写器

**三、读写器的IO接口**

①RS-232串行接口：计算机普遍适用的标准串行接口，能够进行双向的数据信息传递。它的优势在于通用、标准，缺点是传输距离不会达到很远，传输速度也不会很快。

②RS-485串行接口：也是一类标准串行通信接口，数据传递运用差分模式，抵抗干扰能力较强，传输距离比RS-232传输距离较远，传输速度与RS-232差不多。

③以太网接口：阅读器可以通过该接口直接进入网络。

④USB接口：也是一类标准串行通信接口，传输距离较短，传输速度较高。

WLAN接口：是无线局域接口。

**四、读写器的发展趋势**

低成本，多功能、多制式兼容、多频段兼容、小型化、多数据接口、便携式、多智能天线端口、嵌入式和模块化。

第六部分 RFID电子标签

**一、RFID电子标签的构成**

****

（1）天线：主要的功能是接收阅读器传送过来的电磁信号或者将阅读器所需要的数据传回给阅读器，也就是负责发射和接收电磁波。它是电子标签与读写器之间联系的重要一环；

**天线的要求**

①体积要足够小，因为天线还要嵌入到体积很小的电子标签中

②要具有全向性，或者覆盖半球的方向性

③要能够为电子标签当中的芯片供给能量，并保证芯片获得的信号最大化

④要保证不管标签的位置在哪里，天线都能够正常的与阅读器进行通信

⑤要具有鲁棒性。

⑥考虑到电子标签的价格，天线的价格也不应过高。

**天线的分类**

①线圈型

②微带贴片天线

③偶极子天线

（2）射频接口：

电压调节单元：主要用来把从读写器接收过来的射频信号转化为直流电源（DC），并且经由其内部的储能装置（大电容）将能量储存起来，再通过稳压电路，以确保稳定的电源供应；

调制解调单元：由控制单元传出的数据需要经过调制单元的调制以后，才能加载到天线上，成为天线可以传送的射频信号，再回传给阅读器；解调单元负责将经过调制的信号加以解调，将载波去除，以获得最初的调制信号

（3）芯片：

存储单元：主要用于存储系统运行时产生的数据或者识别数据等。

逻辑控制单元：负责对读写器传送来的信号进行译码，并且按照读写器的要求回传数据给读写器

**二、电子标签的技术参数**

①能量需求

②传输速率

③读写速度

④工作频率

⑤容量

⑥封装形式

**三、电子标签的发展趋势**

①工作距离更远：

②无线可读写性能更加完善

③更加适合高速移动物体识别

④快速多标签读写功能更加完善

⑤自我保护功能更加完善

⑥标签附属功能更多。

⑦体积更小

⑧成本更低

第七部分 射频数据的完整性

**一、射频数据的完整性基本概念**

**完整性**：指信息未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

**影响信息完整性的主要因素有**：

设备故障、误码（传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码）、人为攻击、计算机病毒等。

**保证信息完整性**：

1. 协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。
2. 纠错编码方法：由此完成检错和纠错功能。最简单和常用的纠错编码方法是奇偶校验法。
3. 密码校验和方法：它是抗篡改和传输失败的重要手段。
4. 数字签名：保障信息的真实性。
5. 公证：请求网络管理或中介机构证明信息的真实性。

**二、RFID系统的数据传输出错**

**当接收读写器发出的命令以及数据信息发生传输错误时，如果被电子标签接收到，可能会导致以下结果：**

1. 电子标签错误的响应读写器的命令；
2. 电子标签的工作状态发生混乱；
3. 电子标签错误的进入休眠状态。

**当电子标签发出的数据发生传输错误时，如果被读写器接收到，可能导致以下结果：**

1. 不能识别正常工作的电子标签，误判电子标签的工作状态；
2. 将一个电子标签判别为另一个电子标签，造成识别错误。

**三、差错控制方式**



(反馈校验方式)

**四、差错控制编码**

**定义：**

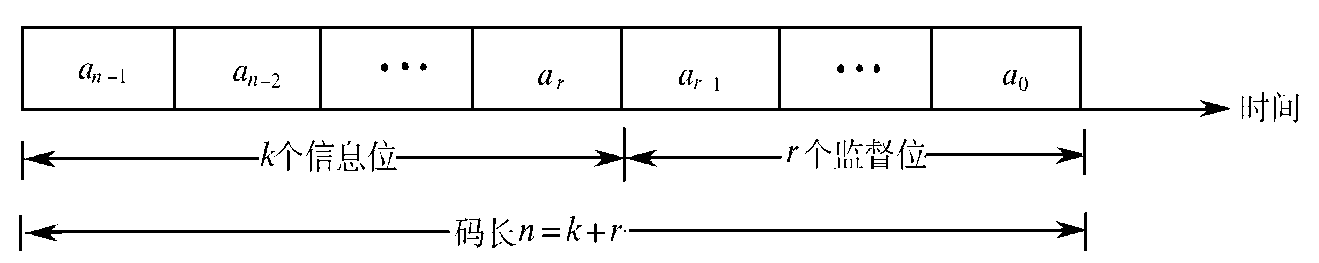
差错控制时所使用的编码，常称为纠错编码。根据码的用途，可分为**检错码**和**纠错码**。检错码以检错为目的，不一定能纠错；而纠错码以纠错为目的，一定能检错。

监督码元：在发送端需要在信息码元序列中增加一些差错控制码元，它们称为监督码元。

**评价标准**

* + 多余度：就是指增加的监督码元多少。例如，若编码序列中平均每两个信息码元就添加一个监督码元，则这种编码的多余度为1/3。
  + 编码效率(简称码率) ：设编码序列中信息码元数量为k，总码元数量为n，则比值k/n 就是码率。
  + 冗余度：监督码元数(n-k) 和信息码元数 k 之比。

**五、汉明码**



* 汉明码又叫**线性分组码**，它是一种能够自动检测并纠正一重错的线性纠错码。
* 汉明码一般可用(n , k)表示。其中，k是每组二进制信息码元的数目，n是编码码组的码元总位数，又称为码组长度，简称码长。n-k=r为每个码组中的监督码元数目。
* 简单地说，汉明码是对每段k位长的信息组以一定的规则增加r个监督元，组成长为*n*的码字。在二进制情况下，共有2*k*个不同的信息组，相应地可得到2*k*个不同的码字，称为许用码组。其余 2*n*-2*k*个码字未被选用，称为禁用码组。
* **码重**：在分组码中，非零码元的数目称为码字的汉明重量， 简称码重。例如，码字 10110，码重*w*=3。
* **码距**：把两个码组中对应位上数字不同的位数称为码组的距离，简称码距。码距又称汉明距离。例如，“000”＝晴，“011”＝云，“101”＝阴，“110”＝雨，4个码组之间，任意两个的距离均为2。再例如 11000 与 10011之间的距离为3。
* **最小码距**：把某种编码中各个码组之间距离的最小值称为最小码距，用*d*０表示。最小码距是码的一个重要参数， 它是衡量码检错、纠错能力的依据。某编码集中的最小码距，被称为系统码距。
* **汉明不等式**：设信息位的个数为k，监督位的个数为r，码长为n=k + r，则汉明不等式为



**举例：**设分组码(n, k)中k = 4，为了纠正1位错码，由上式可知，要求监督位数 r  3。若取 r = 3，则n = k + r = 7。我们用a6 a5 a0表示这7个码元，用S1、S2和S3表示3个监督关系式中的校正子，则S1、S2和S3的值与错码位置的对应关系可以规定如下表所列：

|  |  |  |  |
| --- | --- | --- | --- |
| *S*1 *S*2 *S*3 | 错码位置 | *S*1 *S*2 *S*3 | 错码位置 |
| 001 | *a*0 | 101 | *a*4 |
| 010 | *a*1 | 110 | *a*5 |
| 100 | *a*2 | 111 | *a*6 |
| 011 | *a*3 | 000 | 无错码 |

由表中规定可见，仅当一位错码的位置在a2 、a4、a5或a6时，校正子S1为1；否则S1为零。这就意味着a2 、a4、a5和a6四个码元构成偶数监督关系：



同同理， a1、a3、a5和a6构成偶数监督关系：



及以a0、a3、a4 和a6构成偶数监督关系关系关系



**六、奇偶校验法**

常用的奇偶检验法为**垂直**奇偶校验、**水平**奇偶校验和**水平垂直**奇偶校验。

**七、循环冗余校验（CRC）**

CRC校验码的计算步骤如下：

1. 设G(x)为r阶，在数据块M(x)的末尾附加r个0，则相应的多项式为 ；
2. 按模2除法用对应于G(x)的位串去除对应于 的位串；
3. 按模2减法从对应于 的位串中减去余数（总是小于等于1）。结果就是要传送的带循环冗余校验码的数据块。

下面举个例子来说明一下校验码的计算过程。

* 假设4位的信息位为1010，生成多项式G(x)为 ，那么G(x)的二进制表示形式就为1011，因为G(x)为3阶，所以要在数据块M(x)后面附加3个0，变成1010000。
* 用生成多项式G(x)1011去除1010000，可得余数为011，
* 所以传输的数据块为1010011。

举例：

1、信息码10111001，生成项码10011。

（1）CRC码是多少？（过程不能少）

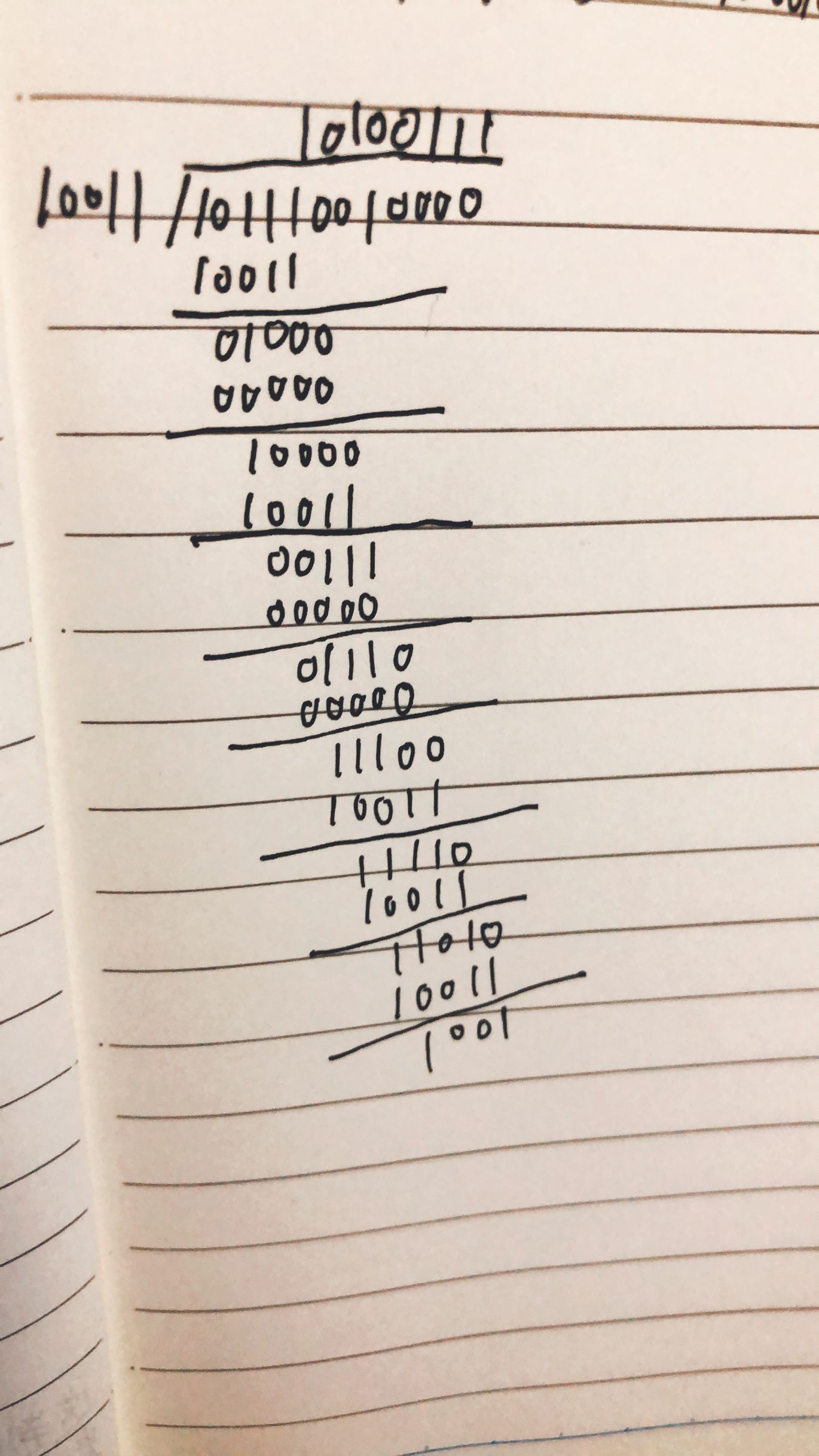
（2）制作（12，8）循环码的出错模式表格（基于生成项码10011）

(1)先在信息码后加4个0，接着模2除法除以生成项码10011，得到余数

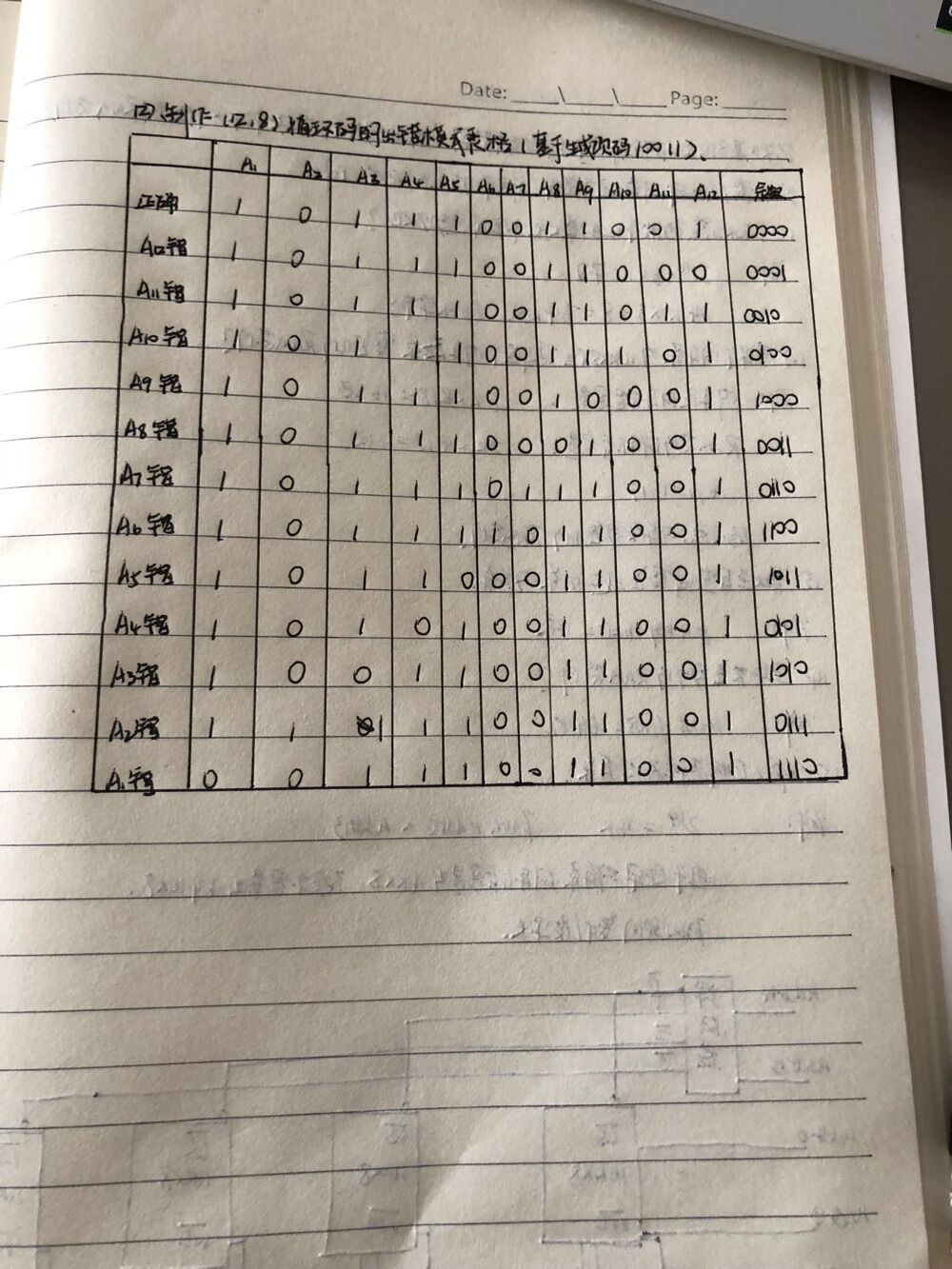
101110010000 / 10011=10100111+1001 / 10011

则CRC码=101110010000+1001=101110011001

竖式见下图：



将上图竖式的被除数换成CRC码，并假设CRC码的最后一位出错，1改成0，利用竖式计算（见PPT），得到第一次的余数，然后继续加0，循环除法可以得到其他位对应的余数，从而可以构建下列表格：



**八、性能指标**

* 射频识别系统的性能指标包括**有效性**、**可靠性**、**适应性**、**标准型**、**经济性**以及**易维护性**等等。
* 在射频识别系统中，识读率PR和误码率PE是用户最为关心的问题。设待识读标签数为NA，正确识读的标签数为NR，每个标签的码元数为NL，读写器识读出发生错误的码元总数为NE，则：



第八部分 射频数据的安全性

**一、射频识别系统的安全分析**

RFID信息系统可能受到的威胁有两类：

物理环境威胁：如电磁干扰、断电、设备故障等威胁；

人员威胁：管理者攻击、用户攻击、前管理者的攻击、前用户攻击、外部人员攻击。

攻击手段：

（1）主动攻击

1.获得RFID标签的实体，通过物理手段在实验室环境中去除芯片封装、使用微探针获取敏感信号、进行目标标签的重构。

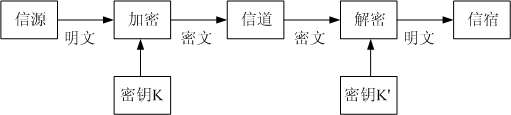
2.用软件利用微处理器的通用接口，扫描RFID标签和响应阅读器的探寻，寻求安全协议加密算法及其实现弱点，从而删除或篡改标签内容。

3.通过干扰广播、阻塞信道或其他手段，产生异常的应用环境，使合法处理器产生故障，拒绝服务器攻击等。

（2）被动攻击

1.采用窃听技术，分析微处理器正常工作过程中产生的各种电磁特征，获得RFID标签和阅读器之间的通信数据。Eg：美国某大学教授和学生利用定向天线和数字示波器监控RFID标签被读取时的功率消耗，通过监控标签的能耗过程从而推导出了密码。根据功率消耗模式可以确定何时标签接收到了正确或者不正确的密码位。

**二、密码学技术原理**

****

常见的密码算法体制有**对称密码体制**和**非对称密码体制**两种。

对称密码体制从得到的密文序列的结构来划分，**有序列密码**和**分组密码**两种不同的密码体制

**三、射频识别系统的加密机制**

在射频识别应用系统上主要采用三种传输信息保护方式，

* 认证传输方式：不保密，纠错
* 加密传输方式：保密，不纠错
* 和混合传输方式：保密，纠错