南京理工大学

2021 年硕士学位研究生入学考试试题

科目代码：878　科目名称：网络空间安全基础　满分：150 分

注意：①认真阅读答题纸上的注意事项；②所有答案必须写在答题纸上，写在本试题纸或草稿纸上均无效；③本试题纸须随答题纸一起装入试题袋中交回！

第一部分：计算机组成原理（共 50 分）

一、 单项选择题：（本题共 9 分，在每小题的四个备选答案中，选出一个正确的答案。）

1、$[X]_{补}=1.X_1X_2X_3X_4$，当满足_____时，X > -1/2 成立。

① $X_1=1$，X_2~X_4 至少有一个为 1　② $X_1=1$，X_2~X_4 任意
③ $X_1=0$，X_2~X_4 至少有一个为 1　④ $X_1=0$，X_2~X_4 任意

2、下列数中最小的数是_____。

① $(100101)_2$　② $(150)_8$　③ $(213)_4$　④ $(625)_{16}$

3、堆栈寻址方式中，设 A 为累加器，SP 为堆栈指示器，M_{SP} 为 SP 指示的栈顶单元。如果出栈操作的动作顺序是（M_{SP}）→A，(SP)+1→SP。那么进栈操作的动作顺序应为_____。

① (A)→M_{SP}，(SP)+1→SP　② (SP)+1→SP，(A)→M_{SP}
③ (SP)-1→SP，(A)→M_{SP}　④ (A)→M_{SP}，(SP)-1→SP

4、主存储器是计算机系统中的记忆设备，它主要用来_____。

① 存放数据　② 存放程序　③ 存放微程序　④ 存放数据和程序

5、以下四种类型指令中，执行时间最长的是_____。

① RR 型指令　② RS 型指令　③ SS 型指令　④ 程序控制指令

6、为了便于实现多级中断，保存现场信息最有效的方式是采用_____。

① 通用寄存器　② 堆栈　③ Cache　④ 磁盘

7、下述 I/O 控制方式中，_____主要由程序实现。

① IOP 方式　② 中断方式　③ DMA 方式　④ 通道方式

8、三种集中式总线控制中，_____方式对电路故障最敏感。

①链式查询　②中断请求　③独立请求　④计数器定时查询

9、在 CPU 中，跟踪后继指令地址的寄存器是_____。

① 指令寄存器　②程序计数器　③地址寄存器　④状态条件寄存器

二、某 16 位计算机的数据通路如图 1.1 所示，其中 M—主存（容量是 $2^{16}\times16$ 位），MBR—主存数据寄存器，MAR—主存地址寄存器，R_0-R_3—通用寄存器，IR—指令寄存器，PC—程序计数器（具有自增能力），C、D--暂存器，ALU—算术逻辑单元(此处做加法器看待)，移位器—左移、右移、直通传送。所有双向箭头表示信息可以双向传送。（本题 11 分）

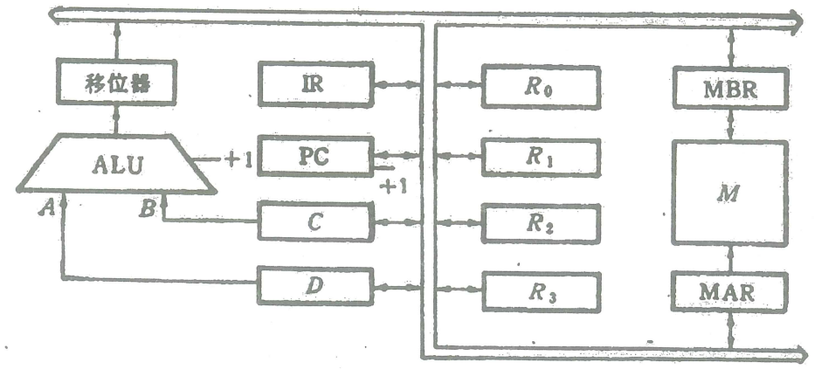

图 1.1 第二题图

说明：

指令：　ADD（R_1），（R_2）+ 的含义是两个数进行求和操作。其中源操作地址在寄存器 R_1 中，目的操作数寻址方式为自增型寄存器间接寻址（先取地址后加 1）。

设 R_1=1000H，主存 1000H 单元的值 2020H，R_2=1002H，主存 1002H 单元的值 1226H

请解答下列问题：

1、按数据通路图画出 ADD 指令的指令周期流程图。（4 分）
2、写出执行 ADD 后，相关寄存器和主存单元值的变化。（4 分）
3、给出执行 ADD 指令访问主存的次数。（3 分）

三、设有一个具有 20 位地址和 32 位字长的存储器，试问：（本题 9 分）

1、该存储器能存储多少个字节的信息？（3 分）
2、如果存储器由 512K×8 位的 SRAM 芯片组成，需多少片？（3 分）
3、若存储器按字编址，则需多少位地址作芯片选择？（3 分）

四、设某计算机中断系统有四个中断源 A、B、C、D（对应的中断请求信号 IRQA、IRQB、IRQC、IRQD 由 D 型触发器锁存），其硬件排队优先次序为 A > B > C > D，现要求将中断处理次序改为 D > A > C > B。请解答下列问题：（本题 10 分）

1．设四个中断源的屏蔽信号为 IMA、IMB、IMC、IMD，并用 D 型触发器保存（0-开放，1-禁止），写出每个中断源对应的屏蔽字。（2 分）

2. 设判优的四个输出信号是 INTA、INTB、INTC、INTD，请画出判优逻辑电路。（判优输入信号由 IREQ_EN=1 控制允许中断请求，判优的基本逻辑器件自己选择使用，但要注明逻辑器件的功能。）（4 分）

3. 按图 1.2 时间轴给出的四个中断源的请求时刻， 画出 CPU 执行程序的轨迹。设每个中断源的中断服务程序时间均为 20μs。（4 分）

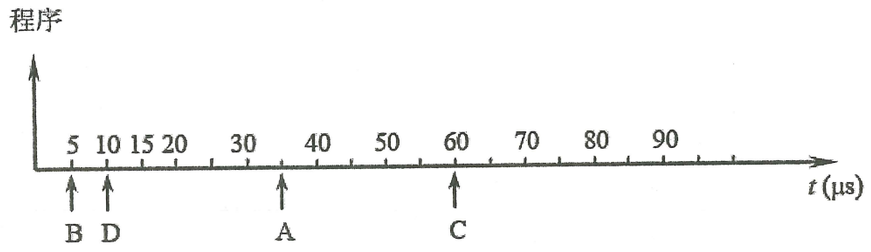

图 1.2 第四题图

五、请回答下列问题（本题 11 分）

1、DRAM 靠的是电容存储，其异步刷新原理是什么？（4 分）

2、在处理器采用流水线工作方式中，存在哪些相关（或障碍）？ 若流水线遇到转移指令，则属于哪种相关？（4 分）

3、微程序控制器设计中字段编码的原则是什么？（3 分）

第二部分：操作系统（共 40 分）

六、单项选择题 (每题 2 分，共 16 分)

1、多个进程之间可能共享_____。

① 地址空间 ② CPU 时间 ③ 外设资源 ④ 内存堆栈

2、进程同步机制应该遵循的准则不包括_____：

① 空闲则入，其他进程均不处于临界区，应允许请求进入临界区的进程进入
② 忙则等待，已有进程处于其临界区，请求进入临界区的进程应等待
③ 有限等待，等待进入临界区的进程不能“死等”
④ 独占等待，不能进入临界区的进程，应暂时占据CPU并转换到阻塞状态

3、作为轻型实体，每个线程拥有有限的少量资源，但不包括_____。

①线程标识符 ②用户栈 ③地址空间 ④核心栈

4、系统中有 3 个不同的临界资源 R1、R2 和 R3，被 4 个进程 p1、p2、p3 及 p4 共享。各进程对资源的需求为：p1 申请 R1 和 R2，p2 申请 R2 和 R3，p3 申请 R1 和 R3，p4 申请 R2。若系统出现死锁，则处于死锁状态的进程数至少是_____。

① 1 ② 2 ③ 3 ④ 4

5、某单 CPU 系统中有输入和输出设备各 1 台，现有 3 个并发执行的作业，每个作业的输入、计算和输出时间均分别为 1 ms、3 ms 和 2 ms，且都按输入、计算和输出的顺序执行，则执行完 3 个作业需要的时间最少是_____。

① 11 ms ② 12 ms ③ 13 ms ④ 14 ms

6、下列关于银行家算法的叙述中，正确的是_____。

① 银行家算法可以预防死锁
② 当系统处于安全状态时，系统中一定无死锁进程
③ 当系统处于不安全状态时，系统中一定会出现死锁进程
④ 银行家算法破坏了死锁必要条件中的请求和保持条件

7、在系统内存中设置磁盘缓冲区的主要目的是_____。

① 减少磁盘 I/O 次数 ② 减少平均寻道时间
③ 提高磁盘数据可靠性 ④ 实现设备无关性

8、某文件系统中，每个文件控制块中采用 8 位二进制串来表示文件的权限，如果文件操作权限分为读、写两种，每类用户对一个文件的访问权限要单独标识，那么最多能支持记录_____类用户。

① 2 ② 3 ③ 4 ④ 8

七、填空题（每个空 1 分，共 5 分）

1、进程间的高级通信可以通过四种形式，即共享存储器、消息传递、_____和客户服务器系统。

2、虚拟存储器借助于利用_____，可以在较小的可用内存中执行较大的用户进程。

3、I/O 系统与高层之间的接口，根据设备类型的不同，可以分为：_____，_____和网络通信接口。

4、磁盘调度算法中，_____算法保证磁盘 I/O 执行顺序为磁盘的 I/O 请求的先后顺序，体现了公平性。

八、名词解释（每个 3 分，共 9 分）

1、并发，并行

2、进程

3、符号链接文件

九、分析简答题（共 10 分）

1、多个进程并发执行时，有可能产生死锁。
1）产生死锁的必要条件都有哪些？（3 分）
2）对应这些死锁条件，可以采用哪些策略来预防死锁的发生？（3 分）

2、假设系统在某时刻有五个进程 P1、P2、P3、P4、P5，共享三类资源 R1、R2、R3，这些资源的总数为 18，6，12。当前时刻的资源分配情况如下：

	已分配资源			资源需求		
	R1	R2	R3	R1	R2	R3
P0	3	2	1	5	5	6
P1	4	0	2	5	3	4
P2	4	0	3	4	5	4
P3	2	0	2	4	5	3
P4	3	1	1	5	1	3

1）此时是否存在一个安全序列，是什么？（2 分）

2）如果 R2 的资源总数减少一些，是否还是可以构成安全序列？保证安全状态的前提下，R3 总数还能减少么？（2 分）

第三部分：现代密码学（共 60 分）

十、单项选择题：(本题共 20 分，每题 2 分)

1、 现阶段加密算法的安全目标是计算上安全，其含义正确的是_____。

① 破译密码所需时间小于被加密信息的有用期
② 破译密码的成本小于被加密信息的价值
③ 破译密码的成本大于被加密信息的价值
④ 破译密码是不可能的

2、 非对称密码算法的加密变换是一个陷门单向函数，其中的陷门是_____。

①公钥　②私钥　③明文　④密文

3、 HMAC 算法可用来生成给定报文的_____。

①散列值　②报文鉴别码　③密文　④报文摘要

4、 下列关于 Kerberos 认证服务中认证符的作用的叙述中，正确的是_____。

①认证符用于证明用户的身份　②认证符可重复使用
③认证符用于安全地分配密钥　④认证符的有效期很长

5、 Feistel 分组密码是几乎所有对称加密算法的基础，在有关 Feistel 分组密码安全性的叙述中错误的是_____。

①分组越大，安全性越高　②密钥越长，安全性越高
③循环次数越少，安全性越高　④子密钥产生算法越复杂，安全性越高

6、 RSA 算法中的密钥长度是指_____。

①公开密钥e的长度　②模数n的长度　③私有密钥d的长度　④e和d长度之和

7、 散列函数生成的报文摘要可用于报文鉴别，下列哪种报文鉴别方案是不安全的_____。

① 使用发送方的私钥加密报文摘要，然后传输报文和加密的报文摘要
② 使用共享密钥加密报文摘要，然后传输报文和加密的报文摘要
③ 在报文摘要生成时引入双方共享的密值，然后传输报文和生成的报文摘要
④ 使用接收方的公钥加密报文摘要，然后传输报文和加密的报文摘要

8、 下列哪个信息没有被包含在 X.509 证书中_____。

①证书持有者　②证书签名值　③私有密钥　④公开密钥

9、 三重 DES：DES-EEE2，其有效密钥长度为_____。

①192　②128　③168　④112

10、 下列关于 AES 加密算法的叙述中，错误的是_____。

① 加密、解密使用相同的算法　② 加密、解密时，密钥使用顺序相反。
③加密、解密时，使用相同的 S 盒子进行替换　④ 加密、解密时，循环移位位数相同

十一、 问答题（30 分）

1、在 HILL 密码体制中，假设密钥为 $K=\begin{bmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{bmatrix}$，请对明文“action”进行加密，写出密文，并对所得密文进行解密，验证加密过程。（6 分）

2、为了适应不同的应用需求，分组密码定义了哪几种操作模式？（6 分）

3、对于 RSA 算法，取 p = 3，q = 11，e = 7。令明文 M = 3，求相应的公钥、私钥以及密文。（6 分）

4、假定 A 从证书权威机构 CA_1 处获得一证书，B 从证书权威机构 CA_2 获得一证书。A、B 可以相互验证对方的证书吗？请详述原因。（6 分）

5、请写出 HMAC 散列函数所生成的报文鉴别码的输出公式，并简要解释其含义。（6 分）

十二、 分析题（10 分）

假定 A 和 B 已经通过某种方法获得了对方的公钥，请利用公钥加密技术，设计个双向身份认证协议。

1、请画出协议的报文交换流程。（5 分）

2、对协议作出简要说明。（5 分）