网安学院 847

847 网络

一、osi 参考模型有哪几层?每一层都有什么功能?(5 分)

二、某信道带宽是 12MHZ,采用 4 级数字信号，最大数据传输率是多少?(默认无噪声环境)三、发送方准备发送 1101011011，若采用 crc 循环冗余码，生成多项式为 x^4+x+1,那么数据传输时的校验码是多少?

四、(15 分）若采用 CSMA/CD，链路长度为 100m,在链路上数据传输速率为 2*10^8m/s,发送方数据发送速率是 1Gbit/s,问当帧长分别为 512B,1500B,64000B,以太网的参数 a 是多少?分别计算信道利用率、吞吐量，并对其分析说明。

五、什么是隐蔽站问题，什么是暴露站问题(5 分)

六、一个 UDP 数据报有效载荷部分为 3192B(固定报头)，现将其经过一个网络进行传送，该网络能通过的最大数据帧长是 1500B，请问应将数据报划分为几个短的数据报分片，通过计算说明 MF,片偏移，分片总长度和数据字段长度并进行填表(行数不够可以手动添加)

原数据报	总长度	数据部分长度	MF	片偏移
分片1				
分片2				
分片3				

七、已知一所学校需要 400 个 ip 地址，平均分配给 4 个机构，向 ISP 申请 IP 地址，ISP 可用的 ip 地址为 202.117.62.0/22，请采用 cidr 技术写出高校所分配到的 ip 地址和其 4 个机构所分配到的 ip 地址块

八、某路由器路由表如下图所示

目的网路	子网掩码	下一跳
202.96.39.0	255.255.255.128	接口m0
202.96.39.128	255.255.255.128	接口m1
202.96.40.0	255.255.255.128	R2
162.4.153.0	255.255.255.192	R3
默认	----------	R4

现收到 5 歌分组他们的目的地址如下 1.202.96.39.10

2.202.96.40.123.202.96.40.151

4.162.153.17(只有三个字段)5.162.4.153.90

分别计算其下–条地址或接

九、解释 TCP 的流量控制和拥塞控制，发送窗口又流量控制决定还是有拥塞控制决定十、FTP 为什么需要两个知名端口号，他们的作用是什么?

847 组原

一、简答题 5 分*6

1.冯诺依曼计算机的特点是什么

2.总线传输分为几个阶段?采用同步定时方式，画出其时序图 3.控制外设输入输出管理的方式有几种?他们有什么特点?

4.有符号定点整数在计算机有那四种表示方式?并对他们进行比较 5.CPU 有哪些寄存器?简述他们的功能

二、计算题(30 分)

1、8 位机器数，最高位为符号位，将-103 用原码，反码，补码，移码表示

1.假设 CPU 执行某段程序是，共访问 cache4800 次，访问主存 200 次，主存的存储周期为 160ns,cache 存取周期是 40ns。

(1)、求 cache/主存系统的命中率(2) 、 cache/主存系统的效率(3)、平均访问时间

2．存储容量 64MB，字长 64 位，模块数为 8，分别采用顺序和交叉方式进行组织。存储周期为 100ns，数据总线宽度为 64 位，总线的传输周期为 t=50ns，那么采用顺序存储和交叉存储带宽各是多少?

3.发出总线申请命令需要 20ns，数据从 DMA 到主存还是从主存到 DMA 时间都是 40ns,采用停止 CPU 访问主存的方式进行数据传输，，数据传输率是 100KB/s,一次传输一个字节，DMA 在传输过程中始终占用总线使用权，问 128 字节块从提出总线申请到传输完毕需要多长时间(数据记不清楚了，题目大体上是这样)

三、分析设计题（15 分)

2、存储字长为 16 位，存储容量为 32K(没有 B)。共有 50 种操作，有页内寻址、直接寻址、间接寻址三种寻址方式，共有 AC、PC、IR、MAR、MDR 这几个寄存器

(还有最后一题分析题，存储容量好像是 64K，不是 32K，最后一个寄存器好像是 MBR，不是 MDR)

(1)、设计指令格式

(2)、该存储器能划分为多少页面，每个页面有多少存储单元(3)、是否可以增加其他寻址方式

未整理信息:

总分 75

一、选择题 10 道，填空题 5 道，每道 2 分，都比较基础，只记得几道

（以下不分选择填空，只算知识点）欧拉函数计算，RSA 公私钥计算，数据加密算法的英文简写，PKI 英文全称（这道是选择题），常见的公钥密码算法，SM4 每轮迭代用几个子密钥，弱碰撞自由的哈希函数和强碰撞自由的哈希函数哪一个安全强度高（填空题），剩下的基本都是概念上的问题，关于 MAC、数字签名之类的概念（不涉及计算）

二、简答题三道（每道 10 分）

1.AES 计算：'B3'+'E4'和'B3'乘'E4'，结果表示成多项式形式（应该是这两个数，反正掌握原理算啥都一样）

注意：题干里给了模数，不用自己背

2.假设攻击者已知密文和加密算法，根据攻击者对资源不同的占有情况，有几种攻击方式，并简单描述。

3.题干给了 Elgmal 签名算法的过程，两问：（1）描述签名的验证过程（2）写出两种 Elgmal 签名算法的变形以及验证过程（其实应该就是 Schnorr 和 DSA，这个可以参考密码学教材）

注意：考纲里面只要求掌握了 RSA 签名算法，如果按考纲来算这题应该算超纲

三、综合题（15 分）

这题没有记得那么仔细，只记得大概，是一道开放性试题，就是选定一个信息系统，分析潜在的风险和利用过程，然后写出涉及到安全的协议中应用到的密码学理论知识（这道题真记不太清了，大概就是这样）