1. 若一无限用户slotted ALOHA信道处于负载不足与过载的临界点，则

(1)信道中空闲时槽的比例是多少？

(2)成功发送一个帧发送次数是多少?(选做，对了加20分)

答：(1)p0=e-G，G=1≡p0(空闲比例)=36.8%

(2)G/S=1/0.368≈2.72(注：S=Ge-G)

2. 简述IEEE 802.3 MAC协议要点(15分)

答：发前监听（CS），边发边听（最小帧长），冲突避让（BEB）

3. 若某站点经历了11次连续冲突，则该次冲突导致站点在IEEE 802.3、802.3u网络中站点的平均等待时间分别为多少？（15分，第1问10分，第2问5分）

答：(1)11>10, (2^10)/2=512;802.3:512\*51.2μs;

(2)802.3u:512\*5.12μs

4. IEEE 802.11协议哪个(或几个)控制帧发现隐藏终端与暴露终端的？(15分, 第1问7.5分，第2问7.5分)

答：(1) 隐藏终端：CTS；

(2)暴露终端：RTS

5. IEEE 802.3 MAC协议中最小帧长的功能与计算依据？(20分)

答：

最小帧长的功能：检测冲突。

计算依据：传输速率\*2\*相距最远的两个站点间传播时延

6.假定生成多项式，试计算帧100110101100 的循环冗余码(CRC)。(15分)

答：11101

7.数字签名是一种可提供发送方身份鉴别、报文完整性和防发送方抵赖的安全机制。(20分)

（1）请给出数字签名最常见的构造方法。

（2）根据数字签名的构造方法，说明数字签名为什么可以提供以上安全服务。

答：

(1) 当实体A需要为报文M生成数字签名时，A首先用一个散列函数计算M的报文摘要，然后用A的私钥加密该报文摘要，生成数字签名。

(2) A的私钥是只有A知道的秘密，任何其它实体无法得到，因而一个有效的数字签名可提供发送方身份鉴别。报文摘要可用于检测报文的完整性，对报文内容的任何修改将产生不同的报文摘要。用A的私钥加密后的报文摘要是不可伪造的，从而数字签名就将A与报文M紧密关联在一起，既能提供报文完整性服务，也能防止发送方抵赖。