**移动通信2020（回忆版）**

1. （1）CBC工作模式加密解密函数（2）为什么这样设计（3）知道密钥不知道IV是否能解密获得完整内容
2. 两个分组加密算法使用同一个密钥；同一个加密算法使用两个密钥；分析哪个安全
3. （1）Diffie-Hellman密钥分配中间人攻击，是否能使用一对公/私钥实现攻击
4. 改进后：双方都使用接收方的公钥进行加密，能否防止中间人攻击
5. 加密，签名，压缩的先后顺序
6. （1）暴露终端，隐藏终端问题描述（2）802.11协议如何解决这个问题
7. （1）分析有线通信和无线通信的安全性（2）TKIP对WEP的改进
8. （1）主动扫描和被动扫描过程描述（2）以及扫描阶段潜在的攻击方式
9. （1）给出单向挑战应答的身份验证过程，如何改进实现双向认证（2）WEP共享密钥方式的漏洞，伪造挑战码应答
10. WEP完整性验证中CRC算法的缺陷，以及改进方式
11. 构造RC4中的密钥K使得KSA步骤的输出S为0-255