**第一章练习题参考答案**

1. **填空：**  
   1. 密码学 密码分析学  
   2. 安全威胁 安全漏洞  
   3. 获取消息的内容 业务流分析  
   4. 被动攻击 主动攻击  
   5. 对信息系统具有摧毁性，故障性，秘密泄漏\_  
   6. 主动攻击  
   7. 中断  
   8. 黑客 恶意代码\_  
   9. 鉴别 访问控制 数据机密性 数据完整性 抗抵赖性(不可否认性)  
   10. 有数据原发证明的抗抵赖 有交付证明的抗抵赖  
   11.鉴别业务（认证业务）  
   12. 对等实体 数据源  
   13. 数据机密性业务  
   14. 访问控制  
   15. 安全通道  
   16. TCP UDP  
   17. 链路加密 端到端加密  
   18. 应用层  
   19. 明文消息空间、密文消息空间、密钥空间、加密变换、解密变换  
   20. 系统的保密性不依赖于对加密体制或算法的保密，仅依赖于密钥的保密性
2. 惟密文攻击、已知明文攻击、选择明文攻击、选择密文攻击
3. 选择明文攻击
4. 密钥
5. **选择**

1-5. AAC （ABC）E

6-10.ACD（ABCDE）D

**三、判断**

**1-5** × × √ √ ×

6-10 × √ √× ×

**四、简答与计算：**

**1 简述安全威胁分类**

业务流分析

中断(可用性)

篡改(完整性)

伪造(真实性)

人为威胁

主动攻击

自然威胁

被动攻击

获取消息内容

安全威胁

**2 消息的安全传输模型中安全通道的作用是什么，与普通的信道有何区别？**

安全通道用于传输秘密参数（会话密钥），是由收发双方共享主密钥建立的。普通信道使用会话密钥加密或认证。  
**3. 在网络中要实现两个实体之间安全的消息传输需要考虑哪4个要素？**  
1）加密、认证算法  
2）用于算法的秘密信息：密钥，秘密参数等  
3）秘密信息的分发与共享：存在秘密信息分发的安全通道（多数情况通过可信第三方来实现或物理手段实现）  
4）使用加密算法和秘密信息以获得安全服务所需要的协议：解决如何安全通信，(加密和认证协议)  
**4.什么是无条件安全和计算安全?**  
无条件安全： 一个加密算法是无条件安全的，如果算法产生的密文不能给出惟一决定相应明文的足够信息。此时无论敌手截获多少密文，花费多少时间，都不能解密密文，即使解出也无法验证结果的正确性(One-Time-Pad)  
计算安全：用已有的最好方法破译该密码系统所需要的努力超过了破译者的破译能力(时间、空间、金钱、设备等)

**5 已知敌手截获了128比特的密文，该密文是用128比特的密钥对128比特的明文加密得到的，请问如果敌手有无限大的计算能力，那么能否破译该密文，为什么？**

不能，仅知道密文，不知道明文任何特征，无法进行有效的惟密文攻击，同时密钥长度与明文长度相同，达到了无条件安全，即使有无限大的计算能力也无法破译。

**6.两种网络加密方式的区别是什么？**  
链路加密是指每个易受攻击的链路两端都使用加密设备进行加密  
 在网络中仅在相邻节点之间加密，数据在该通信链路上的传输是安全的。  
 缺点是在交换机中数据报易受到攻击  
端加密是指仅在一对用户的通信线路两端(即源节点和终端节点)进行加密  
 端到端加密的缺点：容易受业务流量分析的攻击