《现代密码学》课程复习题

题型：简答，填空，选择，判断题，计算，证明，综合题

第一章 绪论

一、填空：

1. 保密学包括两个重要的分支，分别是\_\_\_\_\_\_\_\_\_\_\_\_\_\_和\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. 信息系统产生安全问题的外因是\_\_\_\_\_\_\_\_\_\_\_\_\_内因是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. 信息系统的被动攻击分为哪两类\_\_\_\_\_\_\_\_\_\_\_\_\_\_和\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. 某黑客在信道上截获一段密文后试图破译，这属于哪类威胁\_\_\_\_\_\_\_\_\_\_，该黑客进一步将密文的几个比特改变后转发给收方，这又属于哪类威胁\_\_\_\_\_\_\_

5. 在信息系统的自然威胁中电磁辐射会导致什么问题\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. 攻击者在用户A的主机上种植了盗号木马，并盗取了用户A和用户B的会话密钥，则攻击者使用该密钥以A的身份与B通信的攻击属于哪一类\_\_\_\_\_

7. 攻击者对某服务器发送大量的虚假链接请求，导致该服务器不能向合法用户提供正常服务，这在主动攻击中属于哪一类\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. 人为威胁的主要来源是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_和\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9. 信息系统安全中包含哪5种安全业务\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10. 不可否认业务是指哪两种情况\_\_\_\_\_\_\_\_\_\_\_和\_\_\_\_\_\_\_\_\_\_\_\_

11.为保证通信链接的真实性，通信连接不能被第三方介入，以假冒其中的一方而进行非授权的传输或接受，这需要系统提供哪类安全业务？\_\_\_\_\_\_\_\_\_\_\_\_\_

12. 认证业务可以保证\_\_\_\_\_\_\_\_\_\_的真实性和\_\_\_\_\_\_\_\_\_\_\_的真实性

13. 在收方双方通信时，对发送的消息经常填充一些随机的报文，而在双方通信完毕保持静默的时候，仍然在信道上随机的传送一些消息，这样可提供哪种安全业务\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

14. 在保密系统中，授权用户可以使用授权密钥通过对密文解密来读取消息，而非授权用户则无法读取，那么该系统提供了哪种安全业务\_\_\_\_\_\_\_\_\_\_\_\_\_\_

15. 在信息系统的安全模型中，通信双方共享的秘密信息应采用什么方式传递才是安全的？\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

16. 在TCP/IP协议模型中，传输层的两个协议中\_\_\_\_\_\_\_\_协议是面向连接的，\_\_\_\_\_\_\_协议是面向无连接的

17. 网络加密的基本方式包括\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_和\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

18. 位于两个不同网络中的用户要实现端端安全通信，则可以在OSI的哪些层实现\_\_\_\_\_\_\_\_\_\_

19. 一个密码体制由哪些要素组成\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

20. 在保密通信系统中的基尔霍夫原则是指\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

21. 密码系统有哪些攻击类型?

22. 在密码系统的攻击类型当中，攻击者精心挑选了一段消息，并获得了被攻击者加密的相应密文，则他可以进行哪种攻击？\_\_\_\_\_\_\_\_\_\_\_\_\_

23. 在保密通信系统中，有两个安全的信道，一个是用来安全的传送消息的，另一个是用来传送\_\_\_\_\_\_\_\_\_

二、选择：每一项有1个或多个选项是正确的

1. 下面属被动攻击的有\_\_\_\_\_\_\_\_\_

A. 搭线窃听 B. 对文件或程序非法复制

C. 木马 D. 对资源的非授权使用

2. 将密钥及加密算法封装在硬件芯片中的处理模型属于\_\_\_\_\_\_\_\_

A. 黑盒密码 B. 白盒密码 C. 灰盒密码 D. 可信计算

3. 敌手通过分析某个用户的通信频率来判断该用户的行为，这种攻击属于\_\_\_\_\_

A 内容获取 B重放 C业务流分析 D 篡改

4. 下列哪些类恶意程序需要主程序：

A 逻辑炸弹，B特洛伊木马， C病毒， D蠕虫

5. 下面的安全业务中，那个业务能够保证一个数据不被非授权读取？

A.保密性业务 B.认证性业务 C. 完整性业务 D.不可否认性 E.访问控制

6. 分组密码的差分分析属于\_\_\_\_\_\_\_\_\_\_\_

A 选择明文攻击，B选择密文攻击，C已知明文攻击, D. 惟密文攻击

7. 在选择明文攻击时，除了需要知道加密算法和部分截获的密文以外，还需要知道\_\_\_\_\_\_\_\_\_

A. 不需要知道其它信息； B. 一些明密文对

C. 自己选择的明文消息及由密钥产生的相应密文；

D. 自己选择的密文消息及相应的被解密的明文。

8. 用户的数据要从一个网络传输到另一个网络，则为了实现端到端加密，最低可以在哪一层加密\_\_\_\_\_\_\_

A. 物理层 B. 链路层 C. 网络层 D. 应用层

9. 下面属于用户的隐私的是\_\_\_\_

A 浏览网站的习惯 B 姓名和身份 C 保存的工作单位的机密文档

D. 所在的区域 E 用户是否在某个团队活动区域的附近

10. 下面复杂度属多项式时间复杂度的是

A *O*(1) B *O*(23n) C *O*(2n3) D *O*(n)

三、判断：(正确的划”√”，错误的划”×”，以下同)

1. 某一野战部队通过网络来传送作战指令，那么只要采用安全的密码算法加密，并且保护好密钥就达到保密要求了 （ ）

2. 为了安全的通信，在会话开始前发方随机选择一个安全的密钥通过网络发送给收方，用于对会话的加密 ( )

3. bob设计了一个密码算法，但该算法仅需至少3天时间就可破译，那么bob设计的算法达不到计算安全。 （ ）

4. 一次一密密码系统是无条件安全的 （ ）

5. 安全的杂凑算法都是计算上安全的 （ ）

6. 在保密通信系统中接受者是指所有能够接收到密文的人 ( )

7. 惟密文攻击时只需要知道算法和密文就行了，不需要知道其它信息 （ ）

8. 实现端到端加密一定不能在链路层进行 ( )

9. 链路加密可以保护位于不同路由器的两个用户之间通信的机密性。 ( )

10. 设计密码算法的目标是使其达到完善保密性 ( )

四、简答与计算：

1. 简述安全威胁的分类。

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？

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？

4. 什么是无条件安全和计算安全?

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？

6. 两种网络加密方式的区别是什么？