计算机网络第七章：网络安全 单元测试1

单选题

1. [单选]
网络安全的核心目标之一是保护数据的机密性，这指的是：
（A）确保数据不被篡改
（B）确保数据仅被授权用户访问
（C）确保网络服务正常运行
（D）确保发送者无法否认发送行为

2. [单选]
哪种网络攻击属于主动攻击，通过大量请求耗尽资源，导致服务不可用？
（A）窃听
（B）流量分析
（C）拒绝服务（DoS）
（D）数据篡改

3. [单选]
非法监听网络通信以获取敏感信息，而不对数据进行修改，这属于哪种类型的攻击？
（A）主动攻击
（B）被动攻击
（C）数据篡改
（D）重放攻击

4. [单选]
网络安全的内容之一是身份认证，其目的是：
（A）限制资源访问权限
（B）验证用户或设备身份
（C）保护数据机密性
（D）抵御外部攻击

5. [单选]
数据加密技术中，加密和解密使用同一密钥的是：
（A）对称加密
（B）非对称加密
（C）哈希函数
（D）数字签名

6. [单选]
AES（高级加密标准）是哪种类型加密的常用算法？
（A）非对称加密
（B）哈希函数
（C）数字签名
（D）对称加密

7. [单选]
哪种加密技术使用一对密钥（公钥和私钥），其中一个用于加密，另一个用于解密？
（A）对称加密
（B）非对称加密
（C）数字签名
（D）数据摘要

8. [单选]
数字签名技术主要用于保障数据的什么特性？
（A）机密性和可用性
（B）完整性和认证性
（C）加密性和压缩性
（D）流量控制和差错纠正

9. [单选]
在数字签名过程中，发送者使用什么来加密数据的哈希值（摘要）？
（A）发送者的公钥
（B）接收者的公钥
（C）发送者的私钥
（D）接收者的私钥

10. [单选]
使用指纹或虹膜等生物特征进行身份验证属于哪种认证方法？
（A）基于知识　　（B）基于持有
（C）基于生物特征　　（D）多因素认证

11. [单选]
Kerberos是一种基于对称加密的票据系统，常用于什么环境下的身份认证？
（A）公共互联网上的安全支付　　（B）企业内部网络
（C）无线网络接入　　（D）电子邮件加密

12. [单选]
防火墙是一种网络安全设备或软件，通常部署在网络边界，用于：
（A）加密所有进出数据　　（B）监控和控制进出流量
（C）清除恶意软件　　（D）验证用户身份

13. [单选]
哪种类型的防火墙工作在网络层，基于IP地址、端口等信息进行数据包过滤？
（A）状态检测防火墙　　（B）应用层网关
（C）包过滤防火墙　　（D）下一代防火墙

14. [单选]
防病毒技术中，基于病毒特征库扫描文件以识别已知病毒的技术是：
（A）行为检测　　（B）启发式分析
（C）沙箱技术　　（D）特征码检测

15. [单选]
哪种防病毒技术在虚拟环境中运行可疑程序，观察其行为以识别潜在威胁？
（A）特征码检测　　（B）行为检测
（C）沙箱技术　　（D）启发式分析

判断题

1. [判断]
保护数据的完整性是确保数据仅被授权用户访问。（　　）

2. [判断]
拒绝服务（DoS）攻击是一种被动攻击。（　　）

3. [判断]
网络安全内容中的访问控制是指验证用户或设备的合法性。（　　）

4. [判断]
对称加密算法的计算开销通常大于非对称加密算法。（　　）

5. [判断]
RSA是非对称加密算法的一种。（　　）

6. [判断]
数字签名能够确保数据的机密性。（　　）

7. [判断]
PKI（公钥基础设施）通过数字证书来验证实体身份，广泛用于SSL/TLS安全协议。（　　）

8. [判断]

状态检测防火墙比包过滤防火墙安全性更高，因为它跟踪连接状态。（　　）

9. [判断]

应用层网关（代理防火墙）工作在网络层，速度快但安全性较低。（　　）

10. [判断]

防病毒软件的特征码检测技术可以有效地检测到未知病毒。（　　）

简答题

1. [简答]

请简述网络安全的核心概念“机密性”、“完整性”和“可用性”。

2. [简答]

请简述对称加密和非对称加密的主要区别。