**844《计算机信息安全技术》测试试卷​#（3）**

考试时间：[X] 分钟​

满分：100 分​

一、选择题（每题 2 分，共 30 分）​

1.以下哪种密1码体制属于对称密码体制？（ ）​

A. RSA B. ECC C. AES D. Diffie - Hellman​

2. 密码学中的置换密码属于（ ）。​

A. 古典密码 B. 现代密码 C. 公钥密码 D. 量子密码​

3. 在数字签名中，使用（ ）对消息进行签名。​

A. 发送者的公钥 B. 发送者的私钥 C. 接收者的公钥 D. 接收者的私钥​

4.信息认证的主要目的不包括（ ）。​

A. 验证消息的发送者身份 B. 验证消息内容是否被篡改​

C. 验证消息的完整性 D. 验证消息的保密性​

5. 以下哪种认证方式属于基于生物特征的认证？（ ）​

A. 口令认证 B. 令牌认证 C. 指纹认证 D. 智能卡认证​

6. 计算机病毒的主要特点不包括（ ）。​

A. 传染性 B. 隐蔽性 C. 可预测性 D. 破坏性​

7. 宏病毒通常感染的文件类型是（ ）。​

A. EXE 文件 B. COM 文件 C. DOC 文件 D. SYS 文件​

8. 以下哪种加密算法常用于数据加密和密钥交换，并且安全性基于离散对数问题？（ ）​

A. DES B. 3DES C. IDEA D. Diffie - Hellman​

9. 消息认证码（MAC）是使用（ ）生成的。​

A. 单向散列函数 B. 对称密钥 C. 非对称密钥 D. 数字证书​

10.在身份认证中，一次性口令（OTP）的主要优点是（ ）。​

A. 易于记忆 B. 安全性高 C. 方便输入 D. 无需设备​

11. 计算机病毒按寄生方式主要分为引导型、文件型和（ ）。​

A. 复合型 B. 外壳型 C. 入侵型 D. 源码型​

12. 数字证书的主要作用是（ ）。​

A. 保证数据的完整性 B. 验证用户的身份 C. 实现数据加密 D. 防止病毒感染​

13. 以下哪种技术可以用于检测计算机系统中的病毒？（ ）​

A. 防火墙 B. 入侵检测系统 C. 杀毒软件 D. 数据加密​

14. 哈希函数的一个重要特性是（ ）。​

A. 单向性 B. 可逆性 C. 对称性 D. 非对称性​

15 以下关于计算机病毒预防措施的说法，错误的是（ ）。​

A. 安装杀毒软件并定期更新 B. 不随意打开来历不明的邮件​

C. 定期备份重要数据 D. 经常使用移动存储设备​

二、填空题（每题 2 分，共 20 分）​

1. 密码学中，将明文变换为密文的过程称为（ 加密​ ）。​

2. RSA 算法的安全性基于（ 大整数分解 ）问题。​

3. 信息认证主要包括（ 身份 ）认证和消息认证。​

4. 常见的消息认证方式有消息认证码（MAC）和（ 哈希函数 ）。​

5. 计算机病毒按破坏程度可分为良性病毒和（ 恶性 ）病毒。​

6. 数字签名的主要功能包括防抵赖、认证和（ 完整性 ）。​

7. 对称密码体制中，加密密钥和解密密钥（ 相同 ）。​

8. 基于口令的认证方式中，口令的存储方式通常有明文存储和（ 加密 ）存储。​

9. 病毒的触发机制通常有时间触发、事件触发和（ 条件 ）触发。​

10. 信息安全的三个基本属性是保密性、完整性和（ 可用性 ）。​

三、简答题（每题 10 分，共 30 分）​

1. 简述对称密码体制和非对称密码体制的区别。​

2. 防火墙这种防护方式有它的优势，也有它的局限性。请根据你的使用情况，分析防火墙的局限性。（8分）

3. 列举至少三种计算机病毒的传播途径，并简要说明如何防范计算机病毒。​

四、论述题（20 分）​

随着信息技术的快速发展，计算机信息安全面临着越来越多的挑战。请结合所学知识，论述在当今网络环境下，如何综合运用密码学、信息认证技术和计算机病毒防范措施来保障计算机信息系统的安全。

《计算机信息安全技术》测试试卷参考答案​

一、选择题（每题 2 分，共 30 分）​

1. C 解析：A 选项 RSA、B 选项 ECC、D 选项 Diffie - Hellman 均属于非对称密码体制，AES 是对称密码体制。​

2. A 解析：置换密码是古典密码的一种，通过重新排列明文中字符的位置来加密。​

3. B 解析：数字签名使用发送者的私钥对消息进行签名，接收者用发送者的公钥验证签名。​

4. D 解析：信息认证主要验证消息发送者身份、消息内容完整性及是否被篡改，保密性不是信息认证的主要目的。​

5. C 解析：指纹认证属于基于生物特征的认证，口令认证基于用户输入的字符，令牌认证基于硬件设备，智能卡认证基于智能卡设备。​

6. C 解析：计算机病毒具有传染性、隐蔽性、破坏性，其行为往往不可预测。​

7. C 解析：宏病毒通常感染包含宏代码的 DOC 文件等办公文档。​

8. D 解析：Diffie - Hellman 算法常用于数据加密和密钥交换，安全性基于离散对数问题，DES、3DES、IDEA 不是基于此问题。​

9. B 解析：消息认证码（MAC）使用对称密钥生成，用于验证消息完整性和真实性。​

10. B 解析：一次性口令（OTP）每次使用后即失效，安全性高，不易被破解。​

11. A 解析：计算机病毒按寄生方式分为引导型、文件型和复合型。​

12. B 解析：数字证书主要用于验证用户身份，保证通信双方身份真实性。​

13. C 解析：杀毒软件专门用于检测和清除计算机系统中的病毒。​

14. A 解析：哈希函数具有单向性，从哈希值难以反向推导出原始数据。​

15. D 解析：经常使用移动存储设备可能增加感染病毒风险，应谨慎使用。​

二、填空题（每题 2 分，共 20 分）​

1. 加密​

2. 大整数分解​

3. 身份​

4. 哈希函数（散列函数）​

5. 恶性​

6. 完整性​

7. 相同（或一致）​

8. 加密​

9.条件​

10. 可用性​

三、简答题（每题 10 分，共 30 分）​

1. 称密码体制和非对称密码体制的区别：​

密钥管理：对称密码体制中，加密密钥和解密密钥相同，密钥管理复杂，通信双方需安全交换密钥；非对称密码体制有公钥和私钥，公钥可公开，私钥由用户自己保存，密钥管理相对简单。（4 分）​

加密解密速度：对称密码体制加密解密速度快，适合对大量数据加密；非对称密码体制加密解密速度慢，不适合大量数据加密。（3 分）​

应用场景：对称密码体制常用于数据加密；非对称密码体制常用于数字签名、密钥交换等。（3 分）​

2. 答：防火墙系统有如下的局限性：（每条2分）

1) 传统的防火墙在工作时，入侵者可以伪造数据绕过防火墙或者找到防火墙中可能开启的后门；

2) 防火墙不能防止来自网络内部的袭击。通过调查发现，有将近一半以上的攻击都来自网络内部，对于那些将要泄漏企业机密的员工来说，防火墙形同虚设；

3) 由于防火墙性能上的限制，通常它不具备实时监控入侵的能力；

4) 防火墙不能防御所有新的威胁。防火墙仅仅是一种被动的防护手段，只能用来防备已知的威胁，无法检测和防御最新的拒绝服务攻击(DoS)及蠕虫病毒的攻击。

3.至少三种计算机病毒的传播途径，并简要说明如何防范计算机病毒：​

传播途径：​

网络传播：通过网络共享、电子邮件、即时通讯软件等传播。（2 分）​

移动存储设备传播：如 U 盘、移动硬盘等，病毒可自动运行或通过用户手动复制传播。（2 分）​

文件下载传播：从不可信网站下载感染病毒的文件。（2 分）​

防范措施：​

安装杀毒软件并定期更新：及时查杀新出现的病毒。（1 分）​

谨慎使用网络：不随意打开来历不明的邮件和链接，避免访问不可信网站。（1 分）​

安全使用移动存储设备：使用前先杀毒，不随意共享设备。（1 分）​

定期备份重要数据：以防数据被病毒破坏后可恢复。（1 分）​

四、论述题（20 分）​

在当今网络环境下，如何综合运用密码学、信息认证技术和计算机病毒防范措施来保障计算机信息系统的安全​

密码学方面：​

数据加密：使用对称加密算法（如 AES）对大量数据进行加密存储和传输，确保数据在存储和传输过程中的保密性，防止数据被窃取或篡改。例如，企业数据库中的敏感客户信息可使用 AES 加密存储。（3 分）​

密钥管理：采用非对称加密算法（如 RSA）进行密钥交换，保障对称加密密钥的安全传输。同时，建立完善的密钥管理系统，定期更换密钥，防止密钥泄露。（3 分）​

信息认证技术方面：​

身份认证：综合运用多种身份认证方式，如基于口令、令牌、生物特征等的认证，提高认证的准确性和安全性。例如，银行系统采用指纹认证结合动态口令的方式进行用户登录认证。（3 分）​

消息认证：利用消息认证码（MAC）和哈希函数，对传输的消息进行完整性验证，确保消息未被篡改。在电子商务中，订单信息传输时可使用 MAC 保证其完整性。（3 分）​

计算机病毒防范措施方面：​

安装杀毒软件：部署可靠的杀毒软件，定期进行全盘扫描，实时监控系统活动，及时发现和清除病毒。（2 分）​

网络防护：设置防火墙，阻挡外部非法网络访问和病毒入侵；启用入侵检测系统（IDS），监测网络流量中的异常行为，及时发现病毒传播迹象。（3 分）​

用户安全意识培养：加强用户安全培训，提高用户对病毒的防范意识，如不随意打开可疑邮件、不从不明来源下载软件等。（3 分）​

通过综合运用密码学保障数据保密性和完整性，信息认证技术确保身份和消息的真实性，以及计算机病毒防范措施抵御病毒攻击，多管齐下，可有效保障计算机信息系统在复杂网络环境下的安全。