《计算机信息安全技术》期末考试试卷（样例）​（2）

一、选择题（每题 2 分，共 40 分）​

1. 以下哪种加密算法属于对称加密算法？（ ）​

A. RSA B. ECC C. AES D. DSA​

1. 防火墙的主要功能不包括（ ）​

A. 过滤进出网络的数据 B. 管理进出网络的访问行为​

C. 查杀网络中的病毒 D. 封堵某些禁止的业务​

1. 数字证书的作用是（ ）​

A. 证明用户的身份 B. 对数据进行加密​

C. 防止数据被篡改 D. 以上都是​

1. 以下哪个不是常见的网络攻击手段？（ ）​

A. 口令破解 B. 缓冲区溢出 C. 数据加密 D. 拒绝服务攻击​

1. 入侵检测系统按检测技术可分为（ ）​

A. 异常检测和误用检测 B. 基于主机和基于网络​

C. 实时检测和事后检测 D. 集中式和分布式​

1. 下列哪种技术可以防止网络钓鱼攻击？（ ）​

A. 安装杀毒软件 B. 定期更新系统补丁​

C. 谨慎点击不明链接 D. 使用代理服务器​

1. 操作系统的安全机制不包括（ ）​

A. 用户认证 B. 访问控制 C. 数据加密 D. 进程调度​

1. 以下哪种算法常用于数字签名？（ ）​

A. DES B. MD5 C. SHA - 1 D. RSA​

1. 信息安全的基本属性不包括（ ）​

A. 保密性 B. 完整性 C. 可用性 D. 可扩展性​

1. 网络安全漏洞产生的原因不包括（ ）​

A. 软件设计缺陷 B. 硬件故障​

C. 配置不当 D. 人为疏忽​

1. 以下哪种技术可以实现虚拟专用网络（VPN）？（ ）​

A. 隧道技术 B. 加密技术 C. 身份认证技术 D. 以上都是​

1. 计算机病毒的特征不包括（ ）​

A. 传染性 B. 隐蔽性 C. 破坏性 D. 免疫性​

1. 访问控制的主要任务不包括（ ）​

A. 授权 B. 确定访问权限 C. 实施访问控制策略 D. 数据备份​

1. 以下哪种加密算法安全性最高？（ ）​

A. 凯撒密码 B. 维吉尼亚密码 C. AES D. 置换密码​

1. 防止 SQL 注入攻击的有效方法是（ ）​

A. 使用参数化查询 B. 对用户输入进行过滤​

C. 加强数据库用户管理 D. 以上都是​

1. 信息安全风险评估的方法不包括（ ）​

A. 定性评估 B. 定量评估 C. 半定量评估 D. 随机评估​

1. 以下哪种技术可以防止数据被篡改？（ ） ​

A. 哈希函数 B. 数字水印 C. 加密技术 D. 以上都是​

1. 网络隔离技术的主要目的是（ ）​

A. 防止网络病毒传播 B. 提高网络性能​

C. 保护内部网络安全 D. 实现网络资源共享​

1. 操作系统的安全加固措施不包括（ ）​

A. 关闭不必要的服务 B. 升级操作系统版本​

C. 安装杀毒软件 D. 增加系统内存​

1. 以下哪种技术可以用于防范 ARP 欺骗攻击？（ ）​
2. 静态绑定 IP - MAC 地址 （ARP 欺骗攻击通过伪造 ARP 响应包篡改 IP-MAC 地址映射关系。）

B. 使用防火墙​

C. 安装入侵检测系统 D. 定期更新系统补丁​

二、填空题（每题 2 分，共 20 分）​

1. 信息安全的三个基本目标是保密性、完整性和\_\_\_\_可用性\_\_。​
2. 对称加密算法中，加密和解密使用的密钥是\_\_\_相同\_\_\_的。​
3. 防火墙通常部署在内部网络和外部网络之间。​
4. 数字证书是由\_\_\_CA\_\_\_颁发的。​
5. 入侵检测系统可分为基于主机的入侵检测系统和基于\_\_\_网络\_\_\_的入侵检测系统。​
6. 常见的网络攻击类型有\_\_\_**SQL注入攻击**\_\_\_、\_\_**DDoS攻击**\_\_\_\_和中间人攻击等。​
7. 访问控制的三要素是主体、客体和\_\_\_访问控制策略\_\_\_。​
8. 哈希函数的主要特点是\_\_\_单向性\_\_\_和\_\_\_抗碰撞性\_\_\_。​
9. 操作系统的安全机制主要包括用户认证、\_\_访问控制\_\_\_\_和\_安全审计​
10. 网络安全漏洞扫描工具可分为\_\_\_基于主机\_\_\_扫描工具和\_\_基于网络\_\_\_\_扫描工具。​

三、简答题（每题 10 分，共 30 分）​

1. 简述对称加密算法和非对称加密算法的区别，并分别举例说明常见的算法。​
2. 防火墙有哪些类型？简述其各自的特点和应用场景。​
3. 请简述信息安全风险评估的流程和主要内容。​

流程：资产识别→威胁识别→脆弱性识别→风险分析→风险处置（规避/降低/转移/接受）。

内容：评估资产重要性及敏感性，分类分析威胁，检测脆弱点，计算风险等级，制定控制措施保障安全。

四、计算题（10 分）​

1. 已知凯撒密码的密钥为 3，对明文 “HELLO” 进行加密，求密文。（写出详细计算过程）

《计算机信息安全技术》期末考试试卷（样例）​（2）参考答案

**一、选择题（每题 2 分，共 40 分）**

1. **答案**：C  
   **解析**：A 选项 RSA、B 选项 ECC、D 选项 DSA 均属于非对称加密算法，只有 C 选项 AES 是对称加密算法。对称加密算法加密和解密使用相同密钥，非对称加密算法使用一对密钥（公钥和私钥） 。
2. **答案**：C  
   **解析**：防火墙主要功能是过滤进出网络的数据、管理访问行为、封堵禁止业务。查杀网络中的病毒通常是杀毒软件的功能，并非防火墙的主要功能。
3. **答案**：D  
   **解析**：数字证书可证明用户身份，在加密通信中用于对数据加密，其数字签名技术能防止数据被篡改，所以以上选项都是数字证书的作用。
4. **答案**：C  
   **解析**：口令破解、缓冲区溢出、拒绝服务攻击都是常见的网络攻击手段。而数据加密是保障信息安全的技术，不是攻击手段。
5. **答案**：A  
   **解析**：入侵检测系统按检测技术分为异常检测（基于正常行为模型检测异常行为）和误用检测（基于已知攻击特征检测攻击行为）。B 选项基于主机和基于网络是按检测范围分类；C 选项实时检测和事后检测是按检测时间分类；D 选项集中式和分布式是按系统架构分类。
6. **答案**：C  
   **解析**：网络钓鱼攻击主要通过发送虚假链接等方式诱骗用户输入敏感信息。谨慎点击不明链接可有效防止网络钓鱼攻击。安装杀毒软件主要防病毒，定期更新系统补丁可修复系统漏洞，使用代理服务器主要用于隐藏 IP 等，对防范网络钓鱼效果不明显。
7. **答案**：D  
   **解析**：操作系统安全机制包括用户认证（验证用户身份）、访问控制（控制用户对资源的访问权限）、数据加密（保护数据保密性）等。进程调度是操作系统对进程资源分配和管理的方式，不属于安全机制。
8. **答案**：D  
   **解析**：RSA 算法常用于数字签名，利用私钥签名，公钥验证。A 选项 DES 是对称加密算法，不用于数字签名；B 选项 MD5、C 选项 SHA-1 是哈希函数，用于数据完整性校验，本身不能直接用于数字签名。
9. **答案**：D  
   **解析**：信息安全基本属性为保密性（防止信息泄露）、完整性（确保信息不被篡改）、可用性（保证授权用户能正常访问信息），不包括可扩展性。
10. **答案**：B  
    **解析**：网络安全漏洞产生原因有软件设计缺陷（如程序代码存在漏洞）、配置不当（如网络设备配置错误）、人为疏忽（如用户设置弱密码）。硬件故障一般不会直接导致网络安全漏洞，可能影响系统运行，但不是安全漏洞产生的常见原因。
11. **答案**：D  
    **解析**：隧道技术用于构建 VPN 通信通道，加密技术保障数据传输安全，身份认证技术确保用户合法访问，这三种技术共同实现虚拟专用网络（VPN）。
12. **答案**：D  
    **解析**：计算机病毒具有传染性（能自我复制传播）、隐蔽性（隐藏自身以躲避检测）、破坏性（破坏系统或数据）。病毒本身没有免疫性，不会对自身产生免疫效果。
13. **答案**：D  
    **解析**：访问控制主要任务包括授权（赋予用户访问权限）、确定访问权限（明确用户能访问哪些资源）、实施访问控制策略（按策略控制访问）。数据备份是数据保护措施，不属于访问控制的主要任务。
14. **答案**：C  
    **解析**：凯撒密码、维吉尼亚密码、置换密码都是古典加密算法，安全性较低。AES（高级加密标准）是现代对称加密算法，安全性较高，被广泛应用于各种加密场景。
15. **答案**：D  
    **解析**：使用参数化查询、对用户输入进行过滤、加强数据库用户管理都能有效防止 SQL 注入攻击。参数化查询可避免用户输入直接嵌入 SQL 语句；过滤用户输入能防止恶意输入；加强用户管理可限制非法用户操作数据库。
16. **答案**：D  
    **解析**：信息安全风险评估方法有定性评估（基于经验和判断评估风险）、定量评估（用具体数值衡量风险）、半定量评估（结合定性和定量方法），不存在随机评估这种方法。
17. **答案**：D  
    **解析**：哈希函数可通过计算哈希值检测数据是否被篡改；数字水印可嵌入信息到数据中，用于追踪数据篡改；加密技术对数据加密，篡改后密文会变化，能发现数据被篡改，所以以上技术都可防止数据被篡改。
18. **答案**：C  
    **解析**：网络隔离技术主要目的是保护内部网络安全，通过隔离减少外部网络对内部网络的威胁，防止网络攻击和数据泄露等。防止网络病毒传播是其部分作用，但不是主要目的；提高网络性能、实现网络资源共享不是网络隔离技术的主要目的。
19. **答案**：D  
    **解析**：关闭不必要的服务可减少安全风险；升级操作系统版本可修复漏洞；安装杀毒软件可防范病毒入侵，这些都是操作系统的安全加固措施。增加系统内存主要是提升系统运行性能，与安全加固无关。
20. **答案**：A  
    **解析**：ARP 欺骗攻击通过伪造 ARP 响应包篡改 IP-MAC 地址映射关系。静态绑定 IP-MAC 地址可固定地址映射，防止 ARP 欺骗。防火墙、入侵检测系统、定期更新系统补丁对防范 ARP 欺骗攻击效果不明显。

**二、填空题（每题 2 分，共 20 分）**

1. **答案**：可用性  
   **解析**：信息安全三个基本目标即保密性、完整性和可用性，可用性确保授权用户在需要时能正常访问信息和使用资源。
2. **答案**：相同  
   **解析**：对称加密算法的特点就是加密和解密使用相同的密钥，这与非对称加密算法相区别。
3. **答案**：内部网络；外部网络  
   **解析**：防火墙通常部署在内部网络和外部网络之间，对进出网络的流量进行控制和过滤，保护内部网络安全。
4. **答案**：认证机构（CA）  
   **解析**：数字证书由认证机构（CA）颁发，CA 对证书申请者身份进行验证，确保证书的真实性和可靠性。
5. **答案**：网络  
   **解析**：入侵检测系统分为基于主机的入侵检测系统（监测主机系统活动）和基于网络的入侵检测系统（监测网络流量） 。
6. **答案**：示例：拒绝服务攻击；口令破解攻击（答案不唯一，常见网络攻击类型如端口扫描攻击、SQL 注入攻击等也可）  
   **解析**：常见网络攻击类型多样，拒绝服务攻击通过耗尽目标资源使其无法正常服务；口令破解攻击尝试获取用户密码。
7. **答案**：访问控制策略  
   **解析**：访问控制三要素是主体（访问资源的用户或进程等）、客体（被访问的资源）和访问控制策略（规定主体对客体的访问权限）。
8. **答案**：单向性；碰撞性（或抗碰撞性）  
   **解析**：哈希函数主要特点是单向性（从哈希值难以反推出原数据）和碰撞性（不同数据产生相同哈希值的概率很低，即抗碰撞性）。
9. **答案**：访问控制；安全审计（顺序可颠倒，部分教材可能还有数据加密等，合理即可）  
   **解析**：操作系统安全机制主要包括用户认证、访问控制（控制用户对系统资源的访问）和安全审计（记录和分析用户操作行为）。
10. **答案**：基于主机；基于网络（顺序可颠倒）  
    **解析**：网络安全漏洞扫描工具分为基于主机的扫描工具（检测主机系统漏洞）和基于网络的扫描工具（检测网络设备和网络服务漏洞）。

**三、简答题（每题 10 分，共 30 分）**

1. **参考答案**：

**区别**：对称加密算法加密和解密使用相同密钥，加密速度快，计算效率高，但密钥管理困难，在网络环境下密钥传输需安全通道。非对称加密算法使用一对密钥（公钥和私钥），公钥公开，私钥保密，密钥管理方便，可实现数字签名，但加密和解密速度相对较慢，计算量较大。

**常见算法示例**：对称加密算法如 AES（高级加密标准），它具有多种密钥长度可选，安全性较高，广泛应用于数据加密存储和传输场景，如硬盘加密、VPN 数据加密等。非对称加密算法如 RSA，基于数论中的一些数学难题，常用于数字签名、密钥交换等场景，如在数字证书认证中用于验证身份和签名。

1. **参考答案**：

**包过滤防火墙**：特点是基于数据包的源地址、目的地址、端口号和协议类型等信息进行过滤，工作在网络层和传输层。优点是处理速度快，对用户透明；缺点是安全性相对较低，不能检测应用层的内容。应用场景适用于对安全性要求不是特别高，网络流量较大，需要快速处理数据包的网络环境，如小型企业网络的边界防护。

**代理防火墙**：特点是代理服务器位于客户机和服务器之间，代替双方进行通信，工作在应用层。优点是能对应用层数据进行深度检测和控制，安全性高；缺点是处理速度较慢，对服务器性能要求高。应用场景适用于对安全性要求高，需要对应用层协议进行严格管控的网络，如金融机构的网络防护。

**状态检测防火墙**：特点是结合了包过滤防火墙和代理防火墙的优点，跟踪连接状态，对数据包进行动态检测，工作在网络层、传输层和部分应用层。优点是安全性高，处理速度快，能适应多种网络环境；缺点是配置相对复杂。应用场景广泛，适用于各类企业网络和数据中心，既能保障安全，又能满足网络性能需求。

1. **参考答案**：

**流程**：首先是资产识别，识别组织内的信息资产，包括硬件、软件、数据、人员等，并确定其价值。其次是威胁识别，分析可能对资产造成威胁的因素，如网络攻击、自然灾害、人为失误等。然后是脆弱性识别，查找资产存在的安全漏洞和弱点。接着进行风险分析，综合考虑资产价值、威胁和脆弱性，评估风险发生的可能性和影响程度。最后是风险处置，根据风险分析结果，选择合适的风险处置策略，如风险规避、风险降低、风险转移、风险接受等，并制定相应的处置措施。

**主要内容**：包括对信息资产的全面评估，明确其重要性和敏感性；对各种威胁进行分类和分析，了解其来源和危害程度；对资产的脆弱性进行检测和评估，确定易受攻击的点；计算风险值，确定风险等级；根据风险等级制定相应的风险控制措施，保障信息系统的安全稳定运行。

**四、计算题（10 分）**

1. **参考答案**：  
   凯撒密码加密规则是将明文字母按照字母表顺序向后移动指定的密钥位数。

字母 H 在字母表中排第 8 位，向后移动 3 位，8 + 3 = 11，第 11 位字母是 K。

* 字母 E 排第 5 位，5 + 3 = 8，第 8 位字母是 H。
* 字母 L 排第 12 位，12 + 3 = 15，第 15 位字母是 O。
* 第二个字母 L 同样处理，结果还是 O。
* 字母 O 排第 15 位，15 + 3 = 18，第 18 位字母是 R。

所以，明文 “HELLO” 加密后的密文是 “KHOOR”