《计算机信息安全技术》期末考试样例试卷​（1）

一、选择题（每题 2 分，共 40 分）​

1. 下列加密算法中，属于非对称加密算法的是（ ）​

A. DES B. AES C. RSA D. RC4​

1. 网络安全中的 “肉鸡” 通常是指被（ ）控制的计算机。​

A. 病毒 B. 黑客 C. 防火墙 D. 合法用户​

1. 操作系统的安全审计功能主要用于（ ）​

A. 优化系统性能 B. 检测系统漏洞​

C. 记录用户操作行为 D. 防止数据丢失​

1. 防火墙最基本的功能是（ ）​

A. 数据加密 B. 过滤网络流量​

C. 查杀病毒 D. 进行入侵检测​

1. 入侵检测系统按数据源可分为基于主机的 IDS 和基于（ ）的 IDS。​

A. 服务器 B. 网络 C. 应用程序 D. 数据库​

1. 在密码学中，用于验证消息完整性的技术是（ ）​

A. 数字签名 B. 加密 C. 哈希函数 D. 密钥交换​

1. 网络安全漏洞按其成因可分为（ ）​

A. 软件漏洞和硬件漏洞 B. 系统漏洞和应用漏洞​

C. 已知漏洞和未知漏洞 D. 以上都是​

1. 操作系统中，用户权限管理的主要目的是（ ）​

A. 提高系统性能 B. 防止用户误操作​

C. 实现访问控制 D. 便于用户管理​

1. 防火墙的访问控制策略一般分为（ ）​

A. 白名单策略和黑名单策略 B. 允许策略和拒绝策略​

C. 静态策略和动态策略 D. 以上都是​

1. 入侵检测系统的主要功能不包括（ ）​

A. 检测入侵行为 B. 阻断入侵行为​

C. 记录入侵事件 D. 生成安全报告​

1. 数字证书的颁发机构是（ ）​

A. CA B. RA C. PKI D. SSL​

1. 网络安全中的 DDoS 攻击是指（ ）​

A. 分布式拒绝服务攻击 B. 拒绝服务攻击​

C. 端口扫描攻击 D. 网络钓鱼攻击​

1. 对称加密算法的特点是（ ）​

A. 加密和解密使用相同的密钥 B. 加密强度高​

C. 密钥管理简单 D. 适合长距离通信​

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. 增加用户数量 D. 强化用户认证​

1. 防火墙按部署位置可分为（ ）​

A. 软件防火墙和硬件防火墙 B. 边界防火墙和内部防火墙​

C. 企业级防火墙和个人防火墙 D. 包过滤防火墙和代理防火墙​

1. 入侵检测系统的检测技术主要有（ ）​

A. 异常检测和误用检测 B. 基于特征的检测和基于行为的检测​

C. 实时检测和事后检测 D. 以上都是​

1. 网络安全中的 VPN 技术主要用于（ ）​？

A. 实现远程访问 B. 提高网络速度​

C. 增强网络安全性 D. 以上都是​

1. 操作系统中，文件的访问控制列表（ACL）用于（ ）​

A. 记录文件的访问历史 B. 定义文件的访问权限​

C. 保护文件的完整性 D. 防止文件被删除​

1. 以下哪种哈希算法的安全性较高？（ ）​

A. MD5 B. SHA - 1 C. SHA - 256 D. CRC32​

1. 网络安全中的 ARP 欺骗攻击主要影响（ ）​

A. 网络层通信 B. 数据链路层通信​

C. 传输层通信 D. 应用层通信​

二、填空题（每题 1 分，共 20 分）​

1. 信息安全的三个基本属性是保密性、完整性和\_\_\_可用性\_\_\_。​
2. 密码学中，将明文转换为密文的过程称为\_\_\_加密\_\_\_。​
3. 网络安全中的端口扫描是通过探测目标主机的\_\_\_端口\_\_\_来发现潜在的安全漏洞。​
4. 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\_\_\_等。​
5. 防火墙的主要技术包括包过滤技术、\_\_\_代理\_\_\_技术和状态检测技术。​
6. 入侵检测系统的三个基本功能模块是数据采集、\_\_\_数据分析\_\_\_和响应处理。​
7. 数字签名的主要作用是保证消息的完整性、\_\_\_身份认证\_\_\_和不可否认性。​
8. 网络安全漏洞的处理方法主要有\_\_\_修复\_\_\_、规避和检测。​
9. 操作系统中，用户账户的安全管理主要包括账户创建、\_\_\_账户权限设置\_\_\_和账户删除。​
10. 网络安全中的 SSL 协议主要用于保障\_\_\_Web\_\_\_通信的安全。​
11. 信息安全的基本属性包括保密性、完整性、\_\_\_可用性\_\_\_、可控性和不可否认性。
12. 常见的网络攻击类型中，\_\_\_拒绝服务（DoS）\_\_\_攻击是指攻击者通过发送大量的请求使目标系统资源耗尽而无法正常服务。
13. 防火墙根据其工作原理可分为包过滤防火墙、\_\_代理\_\_\_\_防火墙和状态检测防火墙。
14. 加密技术分为对称加密和\_\_\_非对称\_\_\_加密两种类型。
15. 在数字签名技术中，使用\_\_\_私\_\_\_密钥进行签名，使用\_\_\_公\_\_\_密钥进行验证。
16. 恶意软件的常见类型有病毒、\_\_\_间谍软件\_\_\_、木马、蠕虫等。
17. 访问控制的三种主要实现方式是自主访问控制、强制访问控制和\_\_基于角色的\_\_访问控制。
18. 为了防止数据在传输过程中被篡改，通常会使用\_\_\_消息认证码（MAC）或哈希函数\_\_\_技术。
19. 安全审计是对系统活动和\_\_\_用户行为\_\_\_进行记录、检查和审核的过程。
20. \_\_\_杀毒软件\_\_\_是一种用于保护计算机免受恶意软件侵害的软件程序。

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优缺点，并举例说明它们在实际应用中的场景。​
2. 请列举三种常见的网络攻击方式，并详细阐述针对每种攻击方式的防范措施。​
3. 防火墙和入侵检测系统在网络安全防护中各自的作用是什么？它们如何协同工作以提高网络的整体安全性？​

四、计算题（10 分）​

1. **已知仿射密码的 加密函数可以表示为：**

****

**明文字母、对应的密文字母是、，请计算密钥，来破译此密码，并给出解密函数。**

《计算机信息安全技术》期末考试试卷参考答案​

一、选择题（每题 2 分，共 40 分）​

1. **答案**：C​

**解析**：RSA 是非对称加密算法，DES、AES、RC4 均为对称加密算法。非对称加密算法使用一对密钥，即公钥和私钥，而对称加密算法加密和解密使用同一密钥。​

1. **答案**：B​

**解析**：“肉鸡” 是被黑客通过各种手段控制的计算机，黑客可利用这些计算机进行恶意活动，如发动攻击、窃取数据等。病毒可能是黑客控制计算机的手段之一，但 “肉鸡” 主要是被黑客控制。​

1. **答案**：C​

**解析**：操作系统的安全审计功能主要用于记录用户在系统中的操作行为，包括登录、文件访问、权限变更等操作，以便在需要时进行追溯和分析，保障系统安全。它并非用于优化系统性能、检测系统漏洞或防止数据丢失。​

1. **答案**：B​

**解析**：防火墙最基本的功能是根据预设的规则对网络流量进行过滤，决定哪些流量可以通过，哪些需要被阻止，从而保护内部网络安全。数据加密、查杀病毒和入侵检测并非防火墙的最基本功能。​

1. **答案**：B​

**解析**：入侵检测系统按数据源可分为基于主机的 IDS 和基于网络的 IDS。基于主机的 IDS 主要监测主机系统的活动，如系统日志、文件访问等；基于网络的 IDS 则监测网络流量，分析数据包特征来检测入侵行为。​

1. **答案**：C​

**解析**：哈希函数用于验证消息完整性，它将任意长度的消息映射为固定长度的哈希值，若消息在传输过程中被篡改，其哈希值会发生变化。数字签名也能保证完整性，但主要强调不可否认性；加密用于保护数据保密性；密钥交换用于安全地交换加密密钥。​

1. **答案**：D​

**解析**：网络安全漏洞按成因可分为软件漏洞和硬件漏洞（如硬件设计缺陷）、系统漏洞（操作系统层面）和应用漏洞（应用程序层面）、已知漏洞（已被发现并公开）和未知漏洞（尚未被发现）。​

1. **答案**：C​

**解析**：操作系统中用户权限管理的主要目的是实现访问控制，即规定不同用户对系统资源（如文件、设备等）的访问权限，防止非法访问，保障系统安全。并非为提高系统性能、防止用户误操作或便于用户管理。​

1. **答案**：D​

**解析**：防火墙的访问控制策略一般分为白名单策略（允许特定对象访问）和黑名单策略（禁止特定对象访问）、允许策略和拒绝策略（明确允许或拒绝某些流量）、静态策略（固定不变）和动态策略（可根据条件变化）。​

1. **答案**：B​

**解析**：入侵检测系统的主要功能包括检测入侵行为、记录入侵事件和生成安全报告。阻断入侵行为通常是入侵防御系统（IPS）的功能，IDS 一般不具备直接阻断入侵的能力。​

1. **答案**：A​

**解析**：数字证书的颁发机构是 CA（认证机构），CA 负责验证申请者身份并颁发数字证书。RA（注册机构）协助 CA 进行用户注册等工作；PKI 是公钥基础设施，是一个包括 CA、证书库等的体系；SSL 是安全套接层协议，用于保障通信安全。​

1. **答案**：A​

**解析**：DDoS 攻击即分布式拒绝服务攻击，通过控制大量的计算机（僵尸网络）向目标服务器发送海量请求，导致服务器瘫痪。拒绝服务攻击（DoS）一般指单机向目标攻击；端口扫描攻击用于探测目标主机开放的端口；网络钓鱼攻击通过欺骗手段获取用户敏感信息。​

1. **答案**：A​

**解析**：对称加密算法的特点是加密和解密使用相同的密钥。其加密强度不一定比非对称加密高，密钥管理相对复杂（需安全传输密钥），在长距离通信中密钥传输存在风险。​

1. **答案**：C​

**解析**：操作系统的安全加固措施包括关闭不必要的服务、升级操作系统版本、强化用户认证等，以提高系统安全性。增加用户数量与安全加固无关，甚至可能因用户管理不善带来安全风险。​

1. **答案**：B​

**解析**：防火墙按部署位置可分为边界防火墙（部署在网络边界，保护内部网络与外部网络之间的安全）和内部防火墙（部署在内部网络，保护内部子网之间的安全）。软件防火墙和硬件防火墙是按实现方式分类；企业级防火墙和个人防火墙是按应用场景分类；包过滤防火墙和代理防火墙是按技术分类。​

1. **答案**：A​

**解析**：入侵检测系统的检测技术主要有异常检测（基于正常行为模型，检测偏离正常的行为）和误用检测（基于已知攻击特征库，检测符合特征的攻击行为）。基于特征的检测属于误用检测，基于行为的检测包含异常检测；实时检测和事后检测是按检测时间分类。​

1. **答案**：D​

**解析**：网络安全中的 VPN 技术主要用于实现远程访问，通过加密通道连接远程用户与内部网络；同时能增强网络安全性，防止数据在传输过程中被窃取或篡改；在一定程度上可优化网络连接，提高网络速度。​

1. **答案**：B​

**解析**：操作系统中，文件的访问控制列表（ACL）用于定义文件的访问权限，详细规定不同用户或用户组对文件的读、写、执行等权限。并非用于记录文件访问历史、保护文件完整性或防止文件被删除。​

1. **答案**：C​

**解析**：SHA - 256 哈希算法的安全性较高，MD5 和 SHA - 1 已被发现存在安全漏洞，CRC32 主要用于数据校验，并非用于安全领域的哈希算法。​

1. **答案**：B​

**解析**：网络安全中的 ARP 欺骗攻击主要影响数据链路层通信。ARP 协议用于将 IP 地址解析为 MAC 地址，ARP 欺骗通过伪造 ARP 响应，篡改目标主机的 ARP 缓存，导致数据链路层通信错误。​

二、填空题（每题 2 分，共 20 分）​

1. **答案**：可用性​

**解析**：信息安全的三个基本属性为保密性（防止信息被未授权访问）、完整性（确保信息不被篡改）和可用性（保证授权用户能正常访问信息）。​

1. **答案**：加密​

**解析**：在密码学中，将明文转换为密文的过程称为加密，反之将密文转换为明文的过程称为解密。​

1. **答案**：端口​

**解析**：网络安全中的端口扫描是通过探测目标主机开放的端口来发现潜在的安全漏洞，不同的服务通常对应不同的端口，通过扫描端口可了解目标主机运行的服务及可能存在的安全风险。​

1. **答案**：安全审计（或数据加密，合理即可）​

**解析**：操作系统的安全机制主要包括用户认证（验证用户身份）、访问控制（控制用户对资源的访问权限）和安全审计（记录用户操作行为），部分教材也将数据加密等列为安全机制。​

1. **答案**：代理​

**解析**：防火墙的主要技术包括包过滤技术（根据数据包的源地址、目的地址、端口等信息进行过滤）、代理技术（通过代理服务器转发数据，隐藏内部网络结构）和状态检测技术（跟踪连接状态，进行更智能的过滤）。​

1. **答案**：数据分析​

**解析**：入侵检测系统的三个基本功能模块是数据采集（收集网络流量、系统日志等数据）、数据分析（分析采集到的数据，判断是否存在入侵行为）和响应处理（对检测到的入侵行为进行响应，如报警、记录等）。​

1. **答案**：身份认证​

**解析**：数字签名的主要作用是保证消息的完整性（防止消息被篡改）、身份认证（验证签名者身份）和不可否认性（签名者无法否认自己的签名行为）。​

1. **答案**：修复​

**解析**：网络安全漏洞的处理方法主要有修复（通过安装补丁等方式修复漏洞）、规避（采取措施避免利用漏洞）和检测（及时发现漏洞）。​

1. **答案**：账户权限设置​

**解析**：操作系统中，用户账户的安全管理主要包括账户创建、账户权限设置（设置用户对系统资源的访问权限）和账户删除。​

1. **答案**：Web​

**解析**：网络安全中的 SSL 协议主要用于保障 Web 通信的安全，它在客户端和服务器之间建立加密通道，保护数据传输的保密性和完整性。​

11.可用性

1. 拒绝服务（DoS）
2. 代理
3. 非对称
4. 私，公
5. 间谍软件
6. 基于角色的
7. 消息认证码（MAC）或哈希函数
8. 用户行为
9. 杀毒软件

三、简答题（每题 10 分，共 30 分）​

1. **参考答案**：​

**对称加密算法**：​

* **优点**：加密和解密速度快，效率高；加密强度较高（在合适的密钥长度下）。例如 AES 算法，广泛应用于数据加密场景，在对大量数据进行加密时，能快速完成加密和解密操作。​
* **缺点**：密钥管理困难，通信双方需通过安全的方式共享密钥，在网络环境下密钥传输存在风险；不适合非对称加密场景，如数字签名。​
* **应用场景**：常用于对大量数据的加密存储和传输，如硬盘加密、VPN 中的数据加密等。​

**非对称加密算法**：​

* **优点**：密钥管理方便，公钥可公开分发，无需担心传输安全；可实现数字签名，用于验证消息的来源和完整性，不可否认性。例如 RSA 算法，常用于数字证书认证、数字签名等。​
* **缺点**：加密和解密速度相对较慢，计算量较大；加密强度依赖于密钥长度，密钥长度增加会导致计算复杂度大幅提高。​
* **应用场景**：主要用于身份认证、数字签名、密钥交换等场景，如在电子商务中，用于验证交易双方身份和保证交易数据的完整性。​

1. **参考答案**：​

* **常见网络攻击方式一：SQL 注入攻击​**
* **防范措施**：对用户输入进行严格过滤，使用参数化查询代替拼接 SQL 语句，避免用户输入的数据直接参与 SQL 语句的构造；加强数据库用户管理，最小化用户权限，只赋予必要的权限；定期对数据库进行安全扫描，及时发现和修复漏洞。​
* **常见网络攻击方式二：DDoS 攻击（分布式拒绝服务攻击）​**
* **防范措施**：购买专业的 DDoS 防护服务，利用专业防护设备和技术对流量进行清洗；增加网络带宽，提高服务器的抗攻击能力；部署流量监测系统，实时监测网络流量，及时发现异常流量并采取措施。​
* **常见网络攻击方式三：网络钓鱼攻击​**
* **防范措施**：加强用户安全意识教育，提高用户对钓鱼邮件、链接的识别能力；安装反钓鱼软件，对可疑的邮件、链接进行拦截；企业加强邮件系统管理，对邮件来源进行严格验证，防止伪造邮件进入。​

1. **参考答案**：​

* **防火墙的作用**：防火墙部署在网络边界，根据预设的访问控制策略对进出网络的流量进行过滤，阻挡外部非法网络访问和攻击，保护内部网络安全；隐藏内部网络结构，防止外部直接探测到内部网络拓扑和主机信息；对网络流量进行审计和记录，便于事后分析。​
* **入侵检测系统的作用**：入侵检测系统实时监测网络流量或主机活动，通过数据分析检测是否存在入侵行为；对检测到的入侵行为进行记录，生成详细的安全报告；及时发出报警，通知管理员采取相应措施。​
* **协同工作方式**：防火墙作为网络安全的第一道防线，阻挡大部分已知的、常规的攻击。入侵检测系统则对防火墙过滤后的流量进行更深入的检测，发现潜在的、复杂的入侵行为。当入侵检测系统检测到入侵行为时，可向防火墙发送指令，让防火墙及时调整访问控制策略，阻断入侵源的连接，从而提高网络的整体安全性。同时，防火墙的审计记录也可为入侵检测系统提供分析数据，两者相互补充，协同工作。​

四、计算题（10 分）​

1. **参考答案**：​

由题意可得如下方程组：

 （2分）

由（2）式-（1）式得



可得,进一步可得，即该加密函数为 （2分）

解密函数为：（2分）



或

或