OSI安全体系结构中，五大类安全服务是指？

鉴别服务，访问控制服务，数据机密性服务，数据完整性服务，抗抵赖性服务

在PPDR模型中，通常由四个主要部分组成？

安全策略，防护，检测，响应

计算机信息系统安全的威胁因素主要有哪些？

（1）直接对计算机系统的硬件设备进行破坏。

（2）对存放在系统存储介质上的信息进行非法获取、篡改和破坏等

（3）在信息传输过程中对信息非法获取、篡改和破坏等。

从技术角度分析引起计算机信息系统安全问题的根本原因是什么？

（1）人为的无意失误

（2）人为恶意攻击

（3）软件设计不完善

信息安全的CIA指的是什么？

C 代表机密性I代表完整性A代表可用性

简述PPDR安全模型的构成要素及运作方式

PPDR模型含安全策略、保护、检测、响应四部分。在策略管控下，用防护工具防风险，借检测工具查状态，出问题及时响应，三者循环保障安全。

计算机信息安全研究的主要内容有哪些？

计算机外部安全；计算机内部安全；计算机网络安全。

计算机信息安全的定义是什么？

信息安全是研究在特定应用环境下，依据特定的安全策略，对信息及其系统实施防护、检测和恢复的科学

计算机安全系统中，人、制度和技术之间的关系如何？

人首位，循规办事，违规生漏；技术需懂行人补漏，重在执行制度

计算机病毒的主要特点?

传染性、隐蔽性、破坏性

拒绝服务攻击（DoS）：通过大量的请求消耗目标服务器的资源，使其无法正常响应合法用户的请求，最终导致服务器瘫痪。

木马攻击：通过植入恶意程序来控制目标系统；

网络钓鱼：通过欺骗手段获取用户的敏感信息；

社交工程攻击：是利用人的心理弱点来获取信息。

应用代理防火墙：工作在应用层，它可以对应用层协议进行深入分析和过滤。

包过滤防火墙：工作在网络层和传输层，主要根据数据包的源 IP 地址、目的 IP 地址、端口号等进行过滤；

状态检测防火墙：工作在网络层和传输层。在包过滤的基础上增加了对连接状态的检测；

网络地址转换防火墙：主要用于实现内部网络和外部网络之间的地址转换。

防火墙的主要功能包括访问控制、包过滤和地址转换。

全量备份：是备份所有数据；

增量备份：只备份自上次备份以来发生变化的数据；

差异备份：是备份自上次全量备份以来发生变化的数据。

数字签名：在电子商务交易中，交易双方可以通过验证对方的数字证书来确认其身份的真实性，防止交易抵赖。

加密技术：主要用于保护数据的保密性和完整性；

防火墙：用于网络访问控制；

入侵检测系统：检测网络中的异常行为和潜在攻击

网络安全检测预评估：发现系统漏洞，评估安全风险，提供安全改进建议

其方法有哪些？：漏洞扫描、渗透测试和安全审计

宏病毒通常感染的文件类型是？

宏病毒主要感染包含宏代码的文件，如 DOC 等办公文档。

VPN 采用的主要技术包括？

隧道技术、加密技术和身份认证技术。

计算机病毒按寄生方式可分为？

引导型病毒、文件型病毒和混合型病毒。混合型病毒兼具引导型病毒和文件型病毒的特点，既可以感染引导扇区，也可以感染可执行文件。

入侵检测系统可分为？

基于主机或网络的入侵检测系统。基于主机的入侵检测系统主要监测主机上的系统活动和文件变化；基于网络的入侵检测系统主要监测网络中的数据包和流量。

电子商务安全的主要威胁包括？

信息泄露、篡改、假冒和抵赖。（信息泄露是指敏感信息被非法获取；篡改是指数据在传输过程中被修改；假冒是指攻击者冒充合法用户进行交易；抵赖是指交易双方否认自己的交易行为。）

计算机病毒的传播途径主要有？应对措施有？

网络、电子邮件和存储设备。安装杀毒软件、不随意打开来历不明的邮件和链接、安全使用移动存储设备

防火墙的体系结构有？

双重宿主主机、屏蔽主机、屏蔽子网。（双重宿主主机体系结构通过一台具有两个网络接口的主机来连接内部网络和外部网络；屏蔽主机体系结构使用一个包过滤路由器和一个堡垒主机来保护内部网络；屏蔽子网体系结构在内部网络和外部网络之间增加了一个屏蔽子网，进一步提高了网络的安全性。）

简述计算机病毒的防治措施？

技术层面：安装杀毒软件并定期更新病毒库，实时监测和查杀病毒。  
管理层面：建立计算机病毒防治管理制度，明确使用规范和应急处理流程。

说明防火墙的工作原理？类型

防火墙基于预设规则，通过检查数据包头部信息（如源地址、目的地址、端口号、协议类型等），对进出网络的数据包进行过滤，以保护内部网络免受外部威胁 。

包过滤防火墙、状态检测防火墙和应用代理防火墙

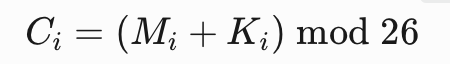
阐述数据备份与恢复的重要性，并举例说明常用的数据恢复场景？

数据备份与恢复可防数据丢失，保障安全与业务连续性。硬件故障，软件错误，人为失误，病毒攻击。

结合实际情况，论述在企业网络环境中，如何综合运用网络攻击与防范技术、入侵检测技术、防火墙技术以及 VPN 技术来构建一个安全可靠的网络架构，保障企业信息安全？

网络攻击与防范技术（加强安全意识培训，采用加密技术，实施访问控制）、入侵检测技术（部署入侵检测系统（IDS）和入侵防御系统（IPS），进行日志分析）、防火墙技术（在企业网络边界部署防火墙，配置防火墙规则）、VPN 技术（采用加密和身份认证技术）

对称加密体制（分组密码体制）：DES、AES。公开密钥加密体制：RSA、NTRU。序列密码体制：RC4

置换密码：天书密码。代换密码：Vigenère(计算方法)

RSA 算法的安全性完全取决于【p、q 的保密性】以及 【大数分解的难度】

请说明研究密码学的意义以及密码学研究内容是什么？

研究密码学能保障信息与系统安全，它分编码与分析，编码保安全，分析攻密码，二者推动其发展。

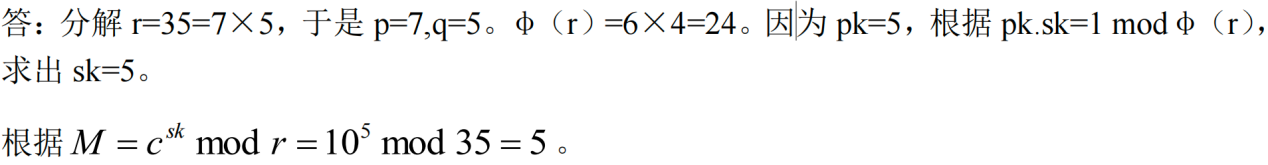
请比较代替密码中移位密码、单表代换密码和多表代换密码的安全性优劣，说明理由？

移位密码仅用一个参数，易遭统计分析攻击；单表代换虽改进，但仍难防此攻击；多表代换用多表组合加密，能消除字母频率特征，有效防止统计分析，安全性较好。

简述序列密码算法与分组密码算法的不同？

分组密码算法是对一个大的明文数据块（分组）进行固定变换的操作；序列密码算法是对单个明文比特的随时间变换的操作。

在一个使用 RSA 的公开密钥系统中，如果攻击者截获了公开密钥 pk=5，公开模数 r=35，密文 c=10，明文是什么？



简述 RSA 算法的优缺点。

优点：RSA 算法的加密密钥和加密算法分开，使得密钥分配更为方便。

缺点：RSA 的 密钥很长，加密速度慢。

在一个使用 RSA 的公开密钥系统中，假设用户的私人密钥被泄露了，他仍使用原来的

模数重新产生一对密钥，这样做安全吗？

安全。当私人密钥被泄漏以后，攻击者只是得到了｛sk，n｝，如果要得到新产生的密钥，

仍然需要进行大数分解才能找到新的密钥，计算难度和破解之前是一样的。

请说明对称密码与公钥密码的主要区别，以及它们的主要应用领域。

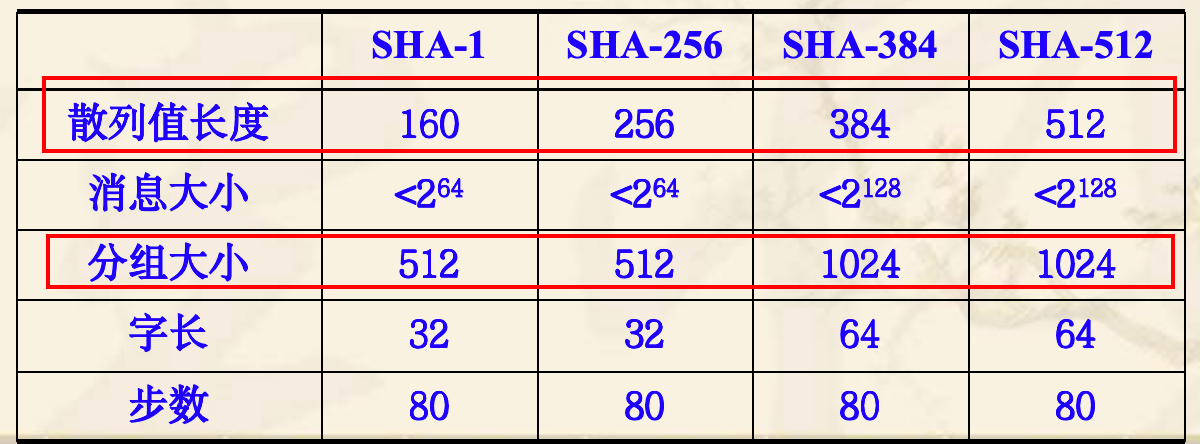
对称密码用同一密钥加密解密，速度快但密钥管理难，用于大量数据加密；公钥密码用公钥加密、私钥解密，安全性高但速度慢，用于数字签名、密钥交换等。

请说明对称密钥与非对称密钥算法中密钥分发的主要区别，以及它们所采用的主要技术

手段？

对称密钥需保密+安全分发，非对称密钥公钥公开，无需额外保护

SHA-1算法：（MD5 和 SHA1 产生的散列值分别是128位和160位）



嗅探器：窃听与分析网络中传输数据包的程序

ARP 欺骗攻击 就是针对 ARP 协议的一种攻击技术，可以造成内部网络的混乱，

让某些被欺骗的计算机无法正常访问网络，ARP 欺骗攻击通过伪造 ARP 响应包篡改 IP-MAC 地址映射关系。

SQL 注入漏洞攻击 是一种比较常见、危害严重的网络攻击，它主要针对 Web 服务

器端的特定数据库系统

目标探测：手动或自动查目标网络的软硬件信息

缓冲区溢出攻击的原理是什么？

黑客会故意塞超量数据，让程序跑偏去执行恶意代码，从而控制你的系统

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？

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。

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。​

**SQL注入攻击**：防措施——过滤输入、参数化查询、最小化权限、定期扫描数据库漏洞。  
**DDoS攻击**：防措施——专业防护服务、扩容带宽、部署流量监测系统。  
**网络钓鱼攻击**：防措施——安全教育、反钓鱼软件、企业邮件验证。

请简述信息安全风险评估的流程和主要内容，重要性。​

流程：资产识别→威胁识别→脆弱性识别→风险分析→风险处置

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。

重要性：信息安全风险评估能识别风险及特性，为策略制定提供依据；明确防护重点、优化资源配置，提高效益；发现漏洞并改进，降低风险，保障系统安全。

防火墙的局限性？

①易被伪造数据绕过或利用后门入侵②无法防御内部攻击③无法实时监控入侵

④无法应对新型攻击

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

①密码学方面：使用对称加密算法进行数据加密，采用非对称加密算法进行密钥管理。②信息认证技术方面：进行身份认证，利用消息认证码（MAC）和哈希函数进行消息认证。③计算机病毒防范措施方面：安装杀毒软件，设置防火墙。④用户安全意识培养

防火墙工作原理？

防火墙是内部与外部网络之间的安全屏障，通过预设策略检查进出数据包（源/目的地址、端口、协议等），决定是否允许通过。

比较包过滤防火墙、状态检测防火墙和应用代理防火墙的特点？

**包过滤防火墙**工作在网络层和传输层，基于数据包头信息过滤，速度快、性能影响小，但无法深度检测应用层数据，安全性较低。

**状态检测防火墙**在包过滤基础上增加连接状态跟踪（如新建、已建立、终止），安全性更高，但对性能有一定影响。

**应用代理防火墙**工作在应用层，通过代理服务深度检测应用层数据，有效防御应用层攻击，但因需逐一代理解析，性能较低且资源消耗大。

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、基于角色的访问控制。

信息安全的基本属性包括？

保密性、完整性、可用性、可控性、不可否认性