第一章

6. 网络空间安全学科的主要研究方向及内容是什么？
9. 信息安全法律法规有几大类别？请举例说明。
10.《中华人民共和国网络安全法》哪一年开始实施？它的实施具有什么意义？

15. 国际上专门从事信息安全通用方法及技术标准化工作的组织是什么？
18. 举例说明中国商用密码标准有哪些。
19. 简述信息安全分级保护和信息安全等级保护。

六、网络空间安全学科的主要研究方向及研究内容

1.密码学

2.网络空间安全

网络空间安全威胁，通信安全，协议安全，网络防护，入侵检测与态势感知，应急响应与灾难恢复，可信网络，网络安全管理

3.系统安全

4.内容安全

5.信息对抗

（通信对抗，雷达对抗，光电对抗，计算机网络对抗）

网络空间安全领域的斗争，本质上都是人与人之间的对抗斗争。

九、三大类别：

国家法律法规，《中华人民共和国宪法》

行政法规，《商用密码管理条例》

部门规范，《信息安全等级保护管理办法》

十、

2017 年 6 月 1 日；意义：解决了我国网络安全“基本法”的问题，我国网络安全工作从此有了基础性的法律框架.

十五、SC27

十八、商用密码标准

（1）SM 系列密码标准

（2）祖冲之密码标准（ZUC）

十九、信息安全标准

1.《涉及国家秘密的 信息系统 分级保护 管理机制》

---涉密信息系统的建设使用单位根据分级保护管理办法和有关标准，对涉密信息系统分等级实施保护

2.《信息系统安全 等级保护 基本要求》

---对组织的信息系统分等级实施保护，对使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应

内容包括：系统定级，系统备案，建设整改，等级测评，监督检查

第二章

2. 请比较恺撒密码、维吉尼亚密码、普莱费尔密码的异同点。
3. 请比较古典密码的置换密码与移位代换密码之间的区别。
5. 为什么说一次一密在理论上安全的？一次一密在实际应用中存在什么问题？
8. Shannon 所提出的设计强密码的思想主要包含哪两个重要的变换？

11. 密码体制从原理上可分为哪两大类？这两类密码体制在密钥的使用上有何不同？

12. 密码分析学是研究分析解密规律的科学，密码攻击有哪些方法？

2、凯撒密码，维吉尼亚密码和普莱费尔密码的异同点：
都是古典密码中的采用位移代换的密码类型，不改变明文顺序，改变明文字母；
不同点在于代换方式不同，凯撒密码采用单表代换；维吉尼亚密码采用多表代换；普莱费尔采用的是多字母代换。
3、古典密码的置换密码和移位代换密码之间的区别：
置换密码不改变明文字母，改变明文顺序
5、若密钥都是真随机数，那么产生的密文流也是真随机数。
问题：
1.产生大规模的随机密钥有困难
2.密钥的分配和保护存在困难
8.shannon 所提出的设计强密码的思想包含
扩散和混淆。

11、密码体制从原理上分为单钥密码体制和双钥密码体制
--单钥密码体制（加密密钥和解密密钥相同）、双钥密码体制（加密和解密分开）
12、密码攻击方法：穷举攻击法、数学攻击法、物理攻击。.

第三章

2. 思考题

(1) 基本的安全威胁有哪些？
(2) 主动攻击和被动攻击有何区别？请举例说明。
(3) 网络攻击的常见形式有哪些？请逐一加以评述。
(4) 请简述安全服务与安全机制之间的关系。
(5) 防火墙一般有几个接口？什么是防火墙的非军事区(DMZ)？它的作用是什么？
(6) 防火墙有什么局限性？只靠防火墙是否能确保某个单位的网络安全？
(7) 入侵检测系统的定义是什么？
(8) 入侵检测系统按照功能可分为哪几类？有哪些主要功能？
(9) 简述 NIDS、HIDS 和 DIDS 三种类型 IDS 之间的区别。
(10) IPSec VPN 有哪两种工作模式？如何通过数据包格式区分这两种工作模式？
(11) 请比较 TLS VPN 与 IPSec VPN 之间的异同点。
(12) 你认为 IPSec VPN 与 SSL VPN 可以相互替代吗？为什么？
(13)《网络安全法》第二十一条规定，国家实行网络安全等级保护制度。我国的网络安全划分为哪几个安全等级？每个安全等级的划分依据是什么？
(14) 工业互联网属于第几次工业革命？工业互联网有哪些主要特点？
(15) 针对工业互联网的攻击发起点有哪些？有哪些具体威胁？
(16) 物联网感知识别层面临哪些安全挑战？

二、
主动攻击
特性：恶意篡改数据流或伪造数据流等攻击行为

分类：伪装攻击、重放攻击、消息篡改、拒绝服务（阻止或禁止人们正常使用网络服务或者管理通信设备）
被动攻击
特性：对所传输的信息进行窃听和监测
分类：窃听攻击、流量分析

Tip:被动攻击难以检测但是容易阻止，主动攻击容易检测但是难以阻止
四、安全服务和安全机制之间的关系：
安全机制是用来实施安全服务的机制，安全机制既可以是具体的、特定的，也可以是通用的，安全服务是指计算机网络提供的安全防护措施。
五、防火墙的局限性：
1.无法防御内部攻击，
2.对绕过防火墙的连接无用
仅靠防火墙无法保证某单位的网络安全
八、入侵检测系统按照功能可分为哪几类
按数据来源---基于网络的、基于主机的、分布式入侵检测系统
按策略---误用检测、异常检测、完整性分析
九、

NIDS：截获数据包，提取特征并与知识库中已知的攻击签名相比较
HIDS：通过对日志和审计记录的监控分析来发现攻击后的误操作
DIDS：同时分析来自主机系统审计日志和网络数据流

不同点：数据来源不同，实时性不同，误报率不同，价格不同
相同点：都是审计跟踪检测数据 监视入侵活动
十一、比较 TLS VPN 与 IPSes VPN 之间的异同点
相同点：身份验证采用双向身份验证和数字证书
不同点:加密方式不同，安全性不同，可访问性不同，费用不同，安装时间不同，使用难易程度不同，用户群体不同，可伸缩性不同，穿越防火墙可行性
十三、网络分为五个安全保护等级。

第一级：一旦受到破坏会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益的一般网络

第二级：一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全的一般网络

第三级：一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络

第四级：一旦受到破坏会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害的特别重要网络

第五级：一旦受到破坏后会对国家安全造成特别严重危害的极其重要网络

十五、针对工业互联网的攻击发起点有物理层，网络层和控制层，如：硬件入侵，木马病毒，网络攻击社交攻击等

第四章

4. 通过对操作系统内部的进程管理、内存管理、外设管理、文件管理、处理器管理等子系统的运行细节来分析操作系统的行为，这样观察系统的方法是否属于自内观察法？为什么？

5. 涌现性和综合特性都是整体特性，但它们是不同的，请结合实例，分析说明两者的区别。

6. 请以操作系统和机密性为例，分析说明为什么系统的安全性是不可能指望依靠还原论的方法建立起来的。

7. 请分析说明如何借助对人的幸福感的观察去帮助理解操作系统安全性的含意，并以此解释系统化思维的含义。

11. 请以 Adept-50 安全操作系统作为分析的例子，分析说明威胁、风险、攻击、安全之间存在什么样的关系。

15. 请分析说明基于特征的入侵检测和基于异常的入侵检测各有什么优缺点，并说明机器学习技术更适合于其中哪类检测。

24. 请分析跨站脚本 XSS 攻击威胁会给 Web 应用系统带来什么样的安全风险。

26.请说出自然生态系统和互联网生态系统的组成部分分别有哪些，并说说如何通过观察前者的相互作用分析后者的相互作用

四、属于自内观察法，因为此时观察者处于系统内对系统进行观察。

综合特性：可以分解为系统组成部分的特性

例：盐的重量

涌现性：不可还原（即不可分解）为系统组成部分的特性

五、 例：盐的毒性

七、系统生命周期的各阶段使命的完成是否有保障如同人生的各个阶段是否平安顺利。

系统思维是一种系统化的思维模式。 从系统整体出发，着眼于系统内部各要素之间连接和相互作用，从整体上去认识局部，再综合到整体。 系统思维其实就是一种观念和意识，做设计决策时要从系统的角度来观察思考，运用系统思维的方法将各项事物有序地组织起来。

十一、安全代表避免伤害，风险代表可能伤害，可见，风险意味着安全难保，所以，风险就是安全风险，即导致安全受损的风险。另一方面，威胁代表产生伤害的意图，给伤害带来可能性，因此，威胁是风险之源。概括地说，威胁引起风险，风险影响安全。故此，需要针对威胁采取措施，降低风险，减少安全损失。

威胁一旦实施，就成了攻击。换言之，攻击(Attack)就是把威胁付诸实施的行为。而攻击的前后经历就是安全事件。攻击如果成功了，威胁所预示的伤害或损失就变成了事实。或者说，安全事件发生后，安全风险就成了实实在在的体现，那便是安全事件所产生的后果。

十五、

基于特征的入侵检测：

优点：较容易检测出已知攻击

缺点：难以检测新的攻击，缺乏新攻击对应的模式

基于异常的入侵检测：
优点：检测未知攻击
缺点：误报问题

机器学习技术适合学习基于异常的入侵检测，机器学习可以根据行为建立模型，在实际应用中，采集可信行为数据是有可能的

二十四、WEB 应用与用户的交互通过输入输出功能实现，用户通过输入输出向应用系统发服务请求，应用系统用输出的形式给用户提供响应结果。在 XSS 攻击中，攻击者想办法把恶意脚本藏在应用的输入输出中，实现攻击目的或者获取用户 cookie。

二十六、

互联网生态系统的组成部分：

1.域名和地址分配
2.开放标准开发
3.全球共享服务和运营
4.用户
5.教育与能力建设
6.地方，地区，国家和全球和全球政策制定

自然界的生态系统

1.无机物
2.有机物
3.环境
4.生产者
5.吞噬生物
6.腐生生物

自然界生态系统的思想表明，生态系统的组成部分相互作用形成统一整体，组成部分间的反馈控制作用维持系统的动态平衡。该思想在网络空间同样适用，它喻示着考虑系统安全问题要注意相互作用和反馈控制。

第五章

10. 描述基于浏览器模拟技术进行网络媒体信息获取过程，分析通过网络交互重构实现网络媒体信息获取的局限性，以及浏览器模拟技术在网络媒体信息获取领域的优势。

21. 请简要说明信息过滤技术有哪些分类与应用。
22. 网络舆情监测与预警系统的核心功能主要包括哪几个方面？
23. 为什么一般的大搜索技术无法完全满足网络舆情监测与预警系统的需求？
24. 未来将影响网络舆情监测与预警系统的技术主要有哪些？
25. 简述内容中心网络的架构有哪些基本组成，并对每一部分进行简要介绍。
26. 简单比较内容中心网络中层次命名和扁平命名的异同，并分别说明这两种命名方式的优缺点。
27. 与经典的 TCP/IP 网络架构相比，内容中心网络架构有哪些不同？又有哪些优势？
28. 针对内容中心网络架构的常见攻击有哪些？简要说明每种攻击方式，并说明这些攻击方式中哪些是专门针对内容中心网络的。

十、基于浏览器模拟实现网络媒体发布信息获取的技术实现过程是，利用典型的 JSSh 客户

端向内嵌 JSSh 服务器的网络浏览器发送 JavaScript 指令，指示网络浏览器开展网页表单自动填写，网页按钮/链接点击，网络身份认证交互，网页发布信息浏览，以及视/音频信息点播等系列操作。

在此基础上，JSSh 客户端进一步要求网络浏览器导出网页文本内容，存储网页图像信息，或在用于信息获取的计算机上对于正在播放的视/音频信息进行屏幕录像，最终面向各种类型的网络内容、各种形态的网络媒体实现发布信息获取。

局限性：新型网络通信协议不断得到应用，部分网络通信协议并不对外公开，无法实现直接通过网络交互重构实现对应协议发布信息获取。

优势：使用便利，节省时间

二十一、

二十二、网络舆情检测与预警系统的核心功能：

1. 高仿真网络信息深度提取技术
2. 基于语义的海量媒体内容特征快速提取与分类技术
3. 非结构信息自组织聚合表达技术

二十三、因为随着互联网的发展，各种良莠不齐的发布内容日渐泛滥。

二十七、

内容中心网络构架的不同：摒弃以 IP 地址为中心的传输架构，采用以内容名称为中心的传输架构。

优势：快速高效的数据传输和增强的可靠性

二十八、

1.命名相关攻击

监视列表攻击

嗅探攻击

2.路由相关攻击

DDOS 攻击

欺骗攻击

3.缓存相关攻击

驱逐流行内容攻击

4.其他攻击

假冒攻击

重放攻击

其中专门针对内容中心网络的是 DDOS

第六章

1. 挑战应答认证协议为什么可以对抗重放攻击？

2. Web 登录认证中经常会碰到输入验证码，它起什么作用？你能否设计一种新的验证码方式？

3. 简述数字证书有效性验证的步骤。

4. FIDO 认证协议的主要目的是什么？简述 UAF 认证的主要流程。

7. 虚拟化主要有哪些方式？其面临的安全威胁是什么？

8. 简述区块链的数据结构，说明其为什么具有不可篡改的特性。

9. 分析比特币采用工作量证明的共识机制与安全性之间的关系。

10. 举例说明人工智能对网络安全的影响。

一、挑战-应答认证方法是通过对一轮应答实现验证者对证明者的认证，利用一次性随机数实现防重放攻击

三、何一个使用证书的第三方在验证证书有效性的时候，要执行以下验证操作：

证书颁发机构是否是其信任的机构。

证书是否在有效期内。

证书是否在证书撤销列表当中。

证书的数字签名是否有效。

所有上述验证通过以后，用户就可以从证书获得证书持有人的公钥，并信任这个公钥。

四、

2. 在线快速身份认证FIDO（Fast Identity Online）：

使用生物特征识别技术代替口令对在线用户进行身份认证，主要思想是基于生物特征识别解锁设备上的加密密钥，使用公钥密码或者对称密码方案与服务器进行身份认证，从而可完全通过本地身份认证实现无口令的登录。

UAF 认证的主要流程是使用者发起申请，APP 要求进行认证。使用者在终端基于存储特征进行认证。

七、虚拟化的实现主要有两种方式：

全虚拟化和硬件支持的虚拟化，对于 IO 虚拟化来说，还有第三种，那就是半虚拟化。

虚拟化面临的安全威胁：

1. 虚拟机逃逸 2.边信道攻击 3.网络隔离 4.镜像和快照的安全

八、区块链的数据结构是由包含交易信息的区块按照从远及近的顺序有序链接起来的。区块被从远及近有序地链接在这个链条里，每个区块都指向前一个区块。

区块链通过密码学哈希函数和非对称加密保证其不可篡改。

十、

作业答案

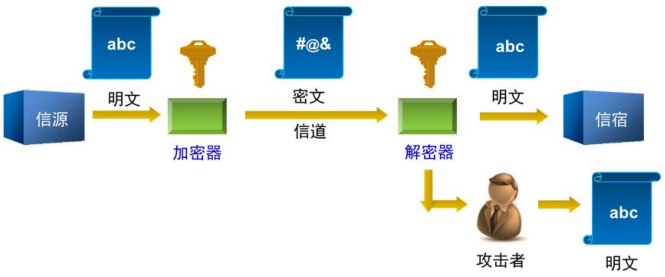
2.1. 古典密码分类与举例。
置换密码：栅格换位、矩形换位。
代换密码：凯撒密码、维吉尼亚密码、普莱费尔密码、弗纳姆密码（基于异或运算）。

2.3. 比较古典密码的置换密码与移位代换密码的区别。
置换密码：不改变明文字符内容，只改变位置。
移位代换密码：不改变明文字符顺序，但改变字符。

2.5. 为什么说一次一密理论上安全？在实际应用中存在什么问题？
密钥永不重复使用，密钥是真随机数。
问题：难以产生大规模随机密钥；密钥需要大量分发，分配和保护存在困难。

2.6. 保密通信系统的数学模型组成。

- 数学模型



2.7. 信息隐藏和信息保密有何本质区别？
加密保护了信息的机密性，隐藏信息真意。
信息隐藏掩盖了发送信息的行为，隐藏信息存在。

2.8. Shannon 提出的设计强密码的思想包含的两个变换。
混淆：将明文及密钥的影响尽可能散布到较多个输出的密文中（代换）。
扩散：使明文和密文之间、密文和密钥之间的统计相关特性极小化（置换）。

2.12. 常见的密码攻击。
穷举攻击法：根据已知信息进行暴力破解。
数学攻击法：分析密码系统所才采用数学变换的特性。
物理攻击法：对密码系统运行中产生的物理量进行分析。

4.3. 操作系统通常由进程管理、内存管理、外设管理、文件管理、处理器管理等子系统组成，是不是把这些子系统的安全机制实现好了,操作系统的安全目标就实现了?为什么?
不是。
还原论存在着局限性，因为，通过对系统组成部分的分析去推知系统的性质这条路并非总是行得通的。系统的某些宏观性质是无法通过其微观组成部分的性质反映出来的。

各子系统的安全机制往往是相互依赖的，需要跨子系统的协同工作才能有效实现整体安全。

4.4. 通过对操作系统内部的进程管理等子系统的运行细节来分析操作系统的行为，是否属于自内观察法？
属于。
自内观察法：位于系统之内对系统进行观察。
自外观察法：观察系统的输入输出来分析系统的行为。

4.6. 请以操作系统和机密性为例,分析说明为什么系统的安全性是不可能指望依靠还原论的方法建立起来的。
操作系统由进程管理、内存管理、外设管理、文件管理及处理器管理等子系统组成。
操作系统的机密性无法还原到子系统之中,即便各子系统都能保证不泄露机密信息,操作系统也无法保证不泄露机密信息。
举例：隐蔽信道泄露。通过系统各个模块或资源之间的隐蔽交互来传递机密信息。例如，进程可能通过共享内存、时间延迟等方式传递信息。

4.9. 请分析说明“失败-保险默认原则”的名称与该原则的实际含义是否吻合。
失败-保险默认原则（Fail-Safe Defults）：为了保险起见，默认让行为失败。
安全机制对访问请求的决定应采取默认拒绝方案。吻合。

4.15. 请分析基于特征和基于异常的入侵检测各有什么优缺点，并说明机器学习更适合哪一类。
基于特征：从已知入侵种提炼特定的模式。比较容易检测出已知攻击，但因缺乏新攻击对应的模式，很难检测出新的攻击。
基于异常：给可信行为建模，出现差异就认为是攻击。可以检测未知攻击，但很容易出现误报。
机器学习模型可以给可信行为建模，更适合应用于后者。

4.18. 请给出用 SHA1 和 strcmp 函数检测代码是否被篡改的方法，然后分析这种方法的不足。
首先用 SHA1 计算程序 P 的摘要,然后用 strcmp 函数比较这个摘要和之前保存的 P 的摘要，如果不一致则认为是篡改了。
SHA1 和 strcmp 本身也是代码程序，如果攻击者有能力篡改程序 P，也有可能篡改了 SHA1 和 strcmp。因此，摘要对比的结果就不可信。

4.19. 请简要说明物理不可克隆函数(PUF)硬件器件主要能提供什么功能,并说说这种硬件器件可用于应对什么安全问题
给定一个输入和相应条件，产生不可预期的唯一输出。
数字指纹：标识硬件身份。
生成唯一性密钥。

4.21. 请分析说明操作系统提供的对文件和内存进行的访问控制有哪些相同和不同之处。
相同之处：基本访问权限相同，读写执行（rwx）。
不同：对文件的访问控制用户看得到，可直接操作；对内存的访问控制是对用户透明的，用

户感受不到。文件访问控制，主体是用户，客体是文件；内存访问控制，主体是进程，客体是内存区域。

4.24. 请分析说明跨站脚本(XSS)攻击威胁会给 Web 应用系统带来什么样的安全风险。
Web 应用与用户的交互通过输入输出功能实现，用户通过输入向应用系统发服务请求，应用系统以输出的形式给用户提供响应结果。
在 XSS 攻击中，攻击者想办法把恶意脚本藏在 Web 应用的输入和输出之中，实现攻击目的。
假设用户 A 和 B 都使用浏览器访问网站 W 提供的 Web 应用系统，XSS 攻击的意思是：A 想攻击 B,A 把实现攻击意图的恶意脚本藏在发给 W 应用系统的输入中，使 W 在不知不觉中把恶意脚本输出给 B,B 的浏览器执行该恶意脚本，无意中帮助 A 实现了攻击 B 的目的。

4.26. 请说出自然生态系统和互联网生态系统的组成部分分别有哪些,并说说如何通过观察前者的相互作用分析后者的相互作用。
生态系统的组成部分包括无机物、有机物、环境、生产者、吞噬生物和腐生生物。
互联网生态系统的组成部分划分为 6 类，分别是：
①域名和地址分配②开放标准开发③全球共享服务和运营。
④用户⑤教育与能力建设⑥地方、地区、国家和全球政策制定。
自然界生态系统的思想表明，生态系统的组成部分相互作用形成统一整体，组成部分间的反馈控制作用维持系统的动态平衡。该思想在网络空间同样适用，它喻示着考虑系统安全问题要注意相互作用和反馈控制。
在网络空间中从生态系统的角度应对系统安全问题，一方面要把系统的概念从传统的意义上拓展到生态系统的范围，重新认识安全威胁，构建相应的安全模型；另一方面要有新的支撑技术，在自动化、互操作性和身份认证等重要关键技术方面有新的突破。

3.2 主动攻击和被动攻击有何区别。
主动攻击：主动攻击是攻击者积极地尝试侵入、破坏或获取系统或网络的未经授权的访问或信息。（主动介入）
伪装、重放、消息篡改、DoS、端口扫描等。
被动攻击：攻击者监视、窃听或分析通信或系统，而不直接干预或影响通信过程。（被动监听）
窃听、流量分析、数据包捕获等。

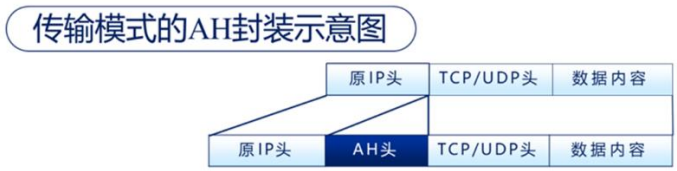
3.3.网络攻击的常见形式有哪些？请逐一加以评述。(P103~107)
口令窃取
欺骗攻击
缺陷和后门攻击
认证失效
协议缺陷
信息泄露
指数攻击——病毒和蠕虫
拒绝服务攻击

3.8. 入侵检测系统按照功能可分为哪几类？有哪些主要功能？

1. 网络入侵检测系统（NIDS，Network-based IDS）：监视网络流量，识别和响应网络中的恶意活动和攻击。
主要功能：检测异常流量模式、分析数据包、识别攻击特征、报警和记录异常活动。
2. 主机入侵检测系统（HIDS，Host-based IDS）：监视单个主机或设备上的活动，检测针对该主机的攻击或异常行为。
主要功能：监视系统日志、文件系统变化、进程活动、注册表变更等，识别异常和潜在攻击。
3. 行为入侵检测系统（BIDS，Behavior-based IDS）：
基于预定义的正常行为模式来检测和识别异常或不寻常的系统或网络活动。
主要功能：建立基线行为、检测异常模式、实时监控系统行为，并触发警报以指示潜在的入侵。
4. 混合入侵检测系统（Hybrid IDS）：结合了多种检测方法和技术，既可以监视网络流量也可以监视主机活动，提供更全面的安全检测和防护。
主要功能：整合网络和主机监视功能，以综合性方式分析和响应潜在的入侵。

3.9. 简述 NIDS、HIDS 和 DIDS 三种类型 IDS 之间的区别。
NIDS：部署在网络边缘或关键网络节点，监视整个网络上的异常流量和攻击行为，如入侵、病毒攻击、DDoS 等
HIDS：部署在单个主机或设备上，监视主机的日志、文件系统、进程等活动，检测针对该主机的攻击或异常行为。
DIDS：由多个 NDS 和 HIDS 组成的分布式系统，覆盖多个网络节点和主机。整合了网络和主机层面的监测功能，提供更全面的安全监控和防护。

3.10. IPSec VPN 有哪两种工作模式？如何通过数据包格式区分这两种工作模式？
传输模式和隧道模式
传输模式：IPSec 对数据包的处理仅涉及到有效负载，只对数据负载进行封装和加密，因此数据包的 IP 头部并不改变。



隧道模式：在隧道模式下，IPSec 对整个 IP 数据包进行封装和加密。IPSec 在原始 IP 数据包外部创建了一个新的 IP 头部和额外的 IPSec 头部，将原始 IP 数据包作为新数据包的负载，整个数据包被加密和封装。（可以认为将原来数据包变成新数据包的数据内容部分）

3.11. 请比较 TLS VPN 与 IPSec VPN 之间的异同点。
相似点
1. 安全性:
TLS VPN 和 IPSec VPN 都提供了加密通信和身份验证，用于保护数据传输的安全性，确保数据在传输过程中的保密性、完整性和可用性。
2. 跨平台支持:
两者都具有跨平台兼容性，能够在多种操作系统和设备上运行并提供安全连接。

三、简述《网络安全法》中关于网络运营者应当履行的网络安全保护义务的主要内容。
《中华人民共和国网络安全法》
第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。
第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

四、请详细阐述并辨析以下两个隐私保护法律法规中的核心概念：“个人数据保护原则”与“数据最小化原则”，并分析它们在隐私保护法律体系中的作用及相互关系。
个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。
个人数据保护原则：在切实保护数据主体的合法权益的原则下,合法,公正,透明地开展对个人数据的流通与处理.
数据最小化原则：在收集数据时，只获取和保留实现特定目的所必需的最少数据量。
个人数据保护原则是隐私保护法律的基础。数据最小化原则的目的是减少隐私泄露或滥用的风险。
数据最小化原则可以看作是个人数据保护原则的一个重要延伸和补充，旨在通过限制数据的收集和使用范围来实现个人数据保护的目标。

6.3. 简述数字证书有效性验证步骤
数字证书→身份认证 P220
验证证书颁发机构是否是其信任的机构
验证证书是否在有效期内
验证证书是否在证书撤销列表中
验证证书的数字签名是否有效

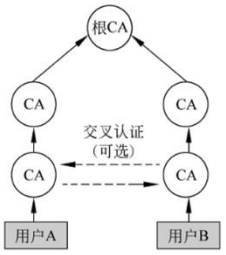
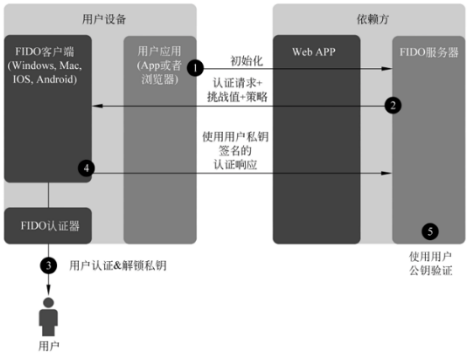


图 6-11 X.509 证书信任体系

6.4. FIDO 认证协议主要目的，UAF 认证流程
认证→身份认证
FIDO 旨在解决在线认证中基于口令认证难题，提供更简单、安全的在线认证方案。P221



6.5.
什么是 k-匿名 P230

6.8.
简述区块链的数据结构，为什么不可篡改
区块链 P246
区块链具有不可篡改性 P250 6.5.5