

测试点1-1

以下描述中体现了信息的何种特性

书中自有黄金屋，书中自有颜如玉

一传十，十传百

没事别翻老黄历

古有飞鸽传书，今有网络通信

兵者诡道也，实则虚之，虚则实之

世间万物皆有运行规律，掌握规律才能使人类与自然和谐共生

信息特性：1.价值性

2.传递性

3.时效性

4.传递性，载体依附性

5.真伪性

6.普遍性

测试点1-2

信息的安全属性在不同应用环境下的重要性（优先级）是不一样的，思考以下应用场景，给出你自己对系统中保密性、完整性和可用性的优先级判断并说明理由。

学校的门户网站，包括院系介绍，教师社区，课程资源等服务内容；

电力部门的输电控制系统，包括电力终端设备状态监控、电力配送调度管理等服务内容；

某研究所的科研成果管理系统，包括产品设计方案管理，实验测试参数管理等服务内容。

学校的门户网站：完整性 可用性 保密性

电力部门的输电控制系统：可用性 完整性 保密性

某研究所的科研成果管理系统：保密性 可用性 完整性

理由：门户网站面向的是全校师生，应该确保使用时的个人信息完整，电力的控制系统控制的是电，是人们的日常生活所需，应该首先保证电力是可以使用的。科研管理成果涉及核心机密，必须首先保证保密性，再考虑可用性和完整性

测试点1-3

场景一：用户A发送文件给用户B。文件中包含需要保护的敏感信息，没有被授权阅读文件的用户C可以监听到文件发送的过程，并在文件传输过程中获得了一份文件的副本。

场景二：网络管理员D发送包含用户授权信息的信息给计算机E，计算机E接收后会 自动更新本地的授权文件。用户F截取了信息，修改后发送给计算机E，后者接收后 认为来自于管理员D，之后相应地更新了授权文件。

问题一：上述场景中何种信息安全属性受到了破坏？

问题二：上述场景中存在的威胁是什么？

问题三：实施的攻击行为属于哪种类型？

问题一： 场景一：真实性，可控性，保密性 场景二： 真实性，可靠性

问题二：人为威胁

问题三：场景一：被动攻击 场景二：主动攻击

测试点1-4

信息安全发展主要经历了哪些阶段，每一阶段的特征和标志性成果是什么？

对信息安全有哪些基本认识？请举例进行说明。

主要阶段：

通信安全：主要标志是 1949年香农发表的《保密通信的信息理论》

主机（计算机）安全：以保密性、完整性和可用性为目标的信息安全阶段。主要标志 1983年美国国防部发布的《可信计算机评估准则》

网络安全：信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为诸如可控性、抗抵赖性、真实性等其他的原则和目标，主要标志是《ISO7498-2- 1989标准》，描述了开放系统互联安全的体系结构。

安全保障：主要标志是美国国家安全局（NSA）1998年制定的《信息保障技术框架》（IATF）

网络空间安全：网络空间是指“构建在信息通信技术基础设施之上的人造空间，用以支撑人们在该空间中开展各类与信息通信技术相关的活动。没有网络安全，就没有国家安全

基本认识：

1.信息安全是相对的，没有绝对的安全；

信息安全没有百分百的安全，就比如每年都有许多互联网公司被曝用户隐私泄露

2.信息安全是一个动态过程，而不是一个产品（或技术）以及多个产品（或技术）的简单堆叠，具有生命周期；

信息安全的发展是一个动态的过程，许多信息安全产品比如说TLS协议，现代密码学的各种加密方式都是在不断进化不断完善的过程，具有一定的生命周期

3.信息安全防护是个全面保护的过程，遵循“木桶原理”，即一个木桶的容积决定于组成它的最短的一块木板，一个系统的安全强度等于它最薄弱环节的安全强度；

信息安全的防护是针对一个系统的防护，它涉及了整个系统的方方面面，比如在公钥加密方式中RSA，敌手可以选择针对N, e, d, m, c进行攻击，但考虑ed的范围较小，许多攻击（共轭，低指数）都会选择短板e和d

4.信息安全包括外部和内部的安全，人是安全机制中最薄弱环节；

信息安全不仅包括外部各种信息系统保护机制方法的安全，也包括人与人之间，人和系统之间的安全，而人因为存在恶性攻击者，成为了安全机制中最薄弱的环节。许多间谍会选择渗透抵抗力的人来获取国家的信息安全机密

5.信息安全是国家安全不可分割的一部分。

没有信息安全，就没有国家安全。信息安全关乎着全国人民的个人隐私，一旦泄露后果不堪设想。美国的棱镜门事件被爆出，可以看到这个国家针对公民隐私的不安全行为

测试点1-5

数据安全与内容安全有什么区别？

举例说明安全服务与安全机制的关系。

移动支付是目前应用最广泛的网络服务之一，以下为消费者在支付过程中的各个环节，请分析在各环节中移动支付系统必须提供的安全服务。

- 数据安全：指对数据收集、存储、检索、传输等过程提供的保护，不被非法冒充、窃取、篡改、抵赖。（处理对象）

内容安全：指依据信息内涵判断是否违反特定安全策略，采取相应的安全措施。（语义内容）

安全服务可以采用一种或多种安全机制来实现，同一种安全机制也可以用于实现不同安全服务。银行为了保证用户的使用安全，会提供健全完善的安全服务，其中就会使用只有个人用户才拥有的password，只有有了password才可以登录。使用password登录就是一种常见的安全机制，它还可以用在QQ，微信，支付系统等不同的安全服务行业。

打开支付终端：访问控制，机密性

扫描支付二维码：完整性

输入支付金额并确认：完整性，机密性

输入支付口令并确认：机密性，完整性，认证

收到支付确认结果：不可否认

测试点1-6

网络空间安全一级学科体系由哪几个研究方向（二级学科）构成？

网络空间安全学科体系结构分为哪几个层次？分别包含哪些研究方向？

二级学科：网络空间安全基础 密码学及应用 系统安全 网络安全 应用安全

层次：

应用层：各种网络空间安全应用技术，电子商务安全、电子政务安全、物联网安全、云计算安全等

技术层：系统安全理论与技术（芯片安全、操作系统安全 数据库安全、中间件安全等），网络安全理论与技术（通信安全、互联网安全、网络对抗、网络安全管理等），

基础层：网络空间理论（网络空间安全体系结构、大数据分析、对抗博弈等），密码学（对称加密、公钥加密、密码分析、侧信道分析等）

测试点1-7

结合“棱镜门事件”，谈谈对“没有网络安全就没有国家安全”的理解。

思考：一名合格的信息安全人才应该具备什么样的素质？

没有网络安全就没有国家安全：

- 1.网络渗透危害政治安全。政治稳定是国家发展、人民幸福的基本前提。当网络安全得不到保证，政治也谈不上稳定，人民也不会幸福。棱镜门虽然只针对美国本土，但很难确定会不会有针对他国的行为。
- 2.国民的个人隐私是至关重要的，棱镜门窃听国民隐私，引发巨大的社会恐慌
- 3.网络安全没有保障，人民的基本权利没有落实，国家也就没有安全

素质：

- 1.保证不使用网络安全做违法犯罪的行为
- 2.从自我做起，勿以恶小而为之
- 3.树立正确的价值观，守法守纪
- 4.确定正确的道德意识，提高道德思想，使用网络信息安全知识造福社会