# 学习笔记3——信息安全和多媒体知识

* 独立完成，不允许抄袭，满分100分；
* 截止日期之前提交至网站作业栏目 ，补交或迟交将被扣分；
* 提交作业后，记得将提交成功的界面截图留证，并重新登录确认是否提交成功。提交失败，且无法提供截图，就会扣分。
* 根据自己的理解，完成作业；
* 文件命名：

上机6\_学习笔记3\_学号\_姓名.docx,例：上机6\_学习笔记3\_12345678\_艾亿.docx

# 第三章 信息安全知识

# 3.1信息安全简介（20分）

根据自己的理解，阐述信息安全；

信息安全主要包括以下五个方面，即需要保证的机密性、真实性、完整性、未授权复制和寄生系统的安全性。信息安全本身涵盖的范围很广，包括如何防止企业机密外泄、防止青少年浏览有害信息、个人信息泄露等。网络环境中的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、消息认证、数据加密等），上至UniNAC、 DLP等，只要存在安全漏洞，就可以威胁到全球安全。信息安全是指信息系统（包括硬件、软件、数据、人员、物理环境及其基础设施）免受意外或恶意原因的破坏、变更或泄露，系统持续、可靠、正常运行。信息服务不中断，最终实现业务连续性。

信息安全学科可以分为两个层次：狭义安全和一般安全。狭义的安全是以密码学为基础的计算机安全领域。中国早期的信息安全专业通常以此为基准，辅以计算机技术和通信网络技术。广义的信息安全是一门综合性学科。从传统的计算机安全到信息安全，不仅是更名，也是安全发展的延伸，安全是一个纯技术问题，而是管理、技术和法律问题相结合的产物。本专业培养可从事计算机、通信、电子商务、电子政务、电子金融等领域的信息安全高级专业人才。

# 3.2密码学简介（20分）

根据自己的理解，阐述密码学（对称密码、公钥密码、散列函数）；

密码术源于将数据传输私有化的需要，因此，在此基础上， 密码术是应用于消息以对其进行加密和解密的方法 这种方式使得该消息的发送者和接收者只能看到纯文本，对于在传输过程中拦截该纯文本的任何人来说，它是完全不可读的，从而足以抵御任何攻击可能会损害正在传输的信息。

对称密码或一键密码-

对称密码术是目前最古老的密码技术，但它仍然提供了很高的安全性。 它基于单个密钥的使用，该密钥将负责加密和解密信息，无论它是使用TLS等协议传输的信息，还是可移动存储设备上的信息。 对称加密是用于加密信息的第一种方法，它基于以下事实：加密和解密都将使用相同的密码，因此，所有想要加密或解密消息的用户都必须拥有此密码。密钥，否则他们将无法执行此操作。 得益于对称密码学，我们可以安全地进行通信或存储文件。

公钥密码-

公钥密码学也称为非对称密码学，基本的意思就是在加密和解密的时候使用不同的秘钥，也就是key ，其中一个是公钥，是可以公开出去的，另外一个是私钥，要严格保密。 但是公钥密码学的应用其实不局限于加密。 公钥密码学要实现的功能有两个：一个是保密，发送者需要是用接收者的公钥去加密信息，接收者就用自己的私钥去解密信息。

单向散列函数-

散列函数是一类将任意长度的输入位(或字节）串转换为固定长度的输出的函数。散列西数的个典型应用是数字签名。给定一个消息 m，当然可以对这个消息本身进行签名。然而，大多数数宁签名方案所采用的公钥运算的运算很大，直接对消息本身签名非常不经济。因此不会直接对 m 进行签名，而是应用散列函数 九，对h (m）进行签名。相对于 成千上万位长度的消息而言，散列西数的输出一般在 128 位到 1024 位之间。对h (m）的签名比对消息 m 的签名要快得多。为保证采取这种方法构造的签名是安全的，必须要求散列西数 万满足以一条件：很难构造两个消息m1和m2，使得 h(m1) =h(m2) 。下面将详细讨论散列西数的安全性质。散列西数有时又称为消息摘要西数，其散列结果也称作摘要或者指纹。散列函数在密码学中有很多应用，它在密码系统中的各个不同部分之间建立紧密的联系。当输入是变长的值时，可以使用散列西数映射为固定长度的值。散列西数可以作为密码学中的伪随机数生成器，从一个共享密钥生成几个密钥。它所具有的单向性也可以起到隔离系统不同部分的作用，以保证即使攻击者得到了其中某个值，也不能获得其他值。

# 3.3自己根据选择的主题命名（自选主题，介绍信息安全的知识，30分）

选择自己感兴趣的主题，介绍信息安全的知识或者新技术，撰写300字~500字。

信息安全特性

-攻防特性：攻防技术交替改进

-相对性：信息安全总是相对的, 够用就行

-配角特性：信息安全总是陪衬角色, 不能为了安全而安全, 安全的应用是先导

-动态性：信息安全是持续过程

信息安全的六个方面

- 保密性（C, confidentiality ）：信息不泄漏给非授权的用户、实体或者过程的特性

- 完整性（I, integrity ）：数据未经授权不能进行改变的特性, 即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性.

- 可用性（A, availability ）：可被授权实体访问并按需求使用的特性, 即当需要时应能存取所需的信息.

- 真实性：内容的真实性

- 可核查性：对信息的传播及内容具有控制能力, 访问控制即属于可控性.

- 可靠性：系统可靠性



图1：信息安全



图2：信息安全

至少要包含2张以上的图片，并利用题注进行编号，在正文对图的引用采用交叉引用的方式。

# 第四章 多媒体知识

# 4.1自己根据选择的主题命名（自选主题，介绍多媒体的知识，30分）

选择自己感兴趣的主题，介绍多媒体的知识或者新技术，撰写300字~500字。

多媒体（Multimedia）是多种媒体的综合，一般包括文本，声音和图像等多种媒体形式。

在计算机系统中，多媒体指组合两种或两种以上媒体的一种人机交互式信息交流和传播媒体。使用的媒体包括文字、图片、照片、声音、动画和影片，以及程式所提供的互动功能。

多媒体技术有以下几个主要特点：

（1）集成性 能够对信息进行多通道统一获取、存储、组织与合成。

（2）控制性 多媒体技术是以计算机为中心，综合处理和控制多媒体信息，并按人的要求以多种媒体形式表现出来，同时作用于人的多种感官。

（3）交互性 交互性是多媒体应用有别于传统信息交流媒体的主要特点之一。传统信息交流媒体只能单向地、被动地传播信息，而多媒体技术则可以实现人对信息的主动选择和控制。

（4）非线性 多媒体技术的非线性特点将改变人们传统循序性的读写模式。以往人们读写方式大都采用章、节、页的框架，循序渐进地获取知识，而多媒体技术将借助超文本链接（Hyper Text Link）的方法，把内容以一种更灵活、更具变化的方式呈现给读者。

（5）实时性 当用户给出操作命令时，相应的多媒体信息都能够得到实时控制。

（6）互动性，它可以形成人与机器、人与人及机器间的互动，互相交流的操作环境及身临其境的场景，人们根据需要进行控制。人机相互交流是多媒体最大的特点。

（7）信息使用的方便性 用户可以按照自己的需要、兴趣、任务要求、偏爱和认知特点来使用信息，任取图、文、声等信息表现形式。

（8）信息结构的动态性 “多媒体是一部永远读不完的书”，用户可以按照自己的目的和认知特征重新组织信息，增加、删除或修改节点，重新建立链接。



图1：多媒体



图2：多媒体

至少要包含2张以上的图片，并利用题注进行编号，在正文对图的引用采用交叉引用的方式。