密 码 学

第一讲　信息安全概论

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室

内容简介

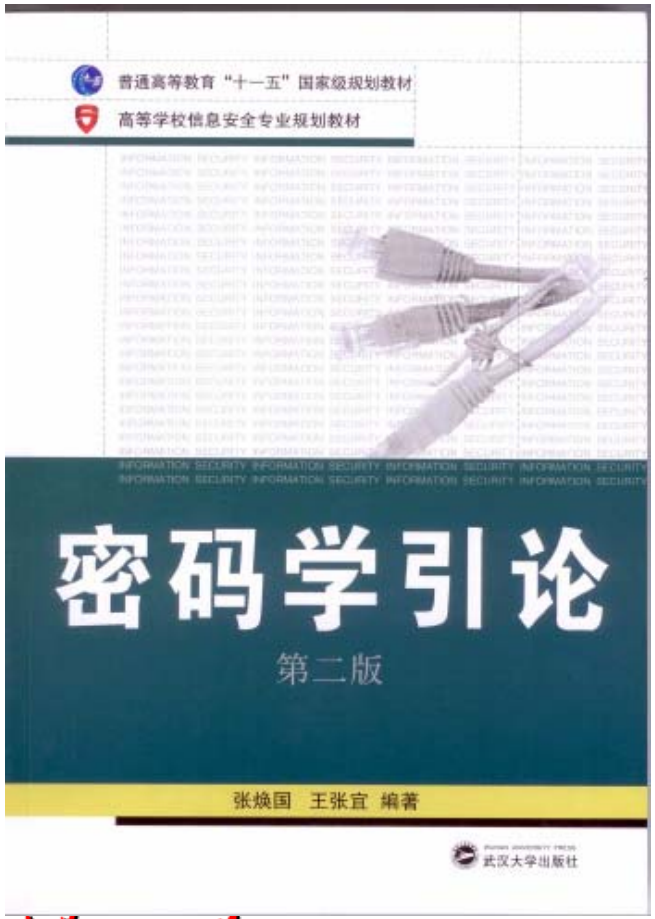
第一讲 信息安全概论
第二讲 密码学的基本概念
第三讲 数据加密标准（DES）
第四讲 高级数据加密标准（AES）
第五讲 中国商用密码（SMS4）
第六讲 分组密码的应用技术
第七讲 序列密码
第八讲 复习
第九讲 公钥密码（1）

内容简介

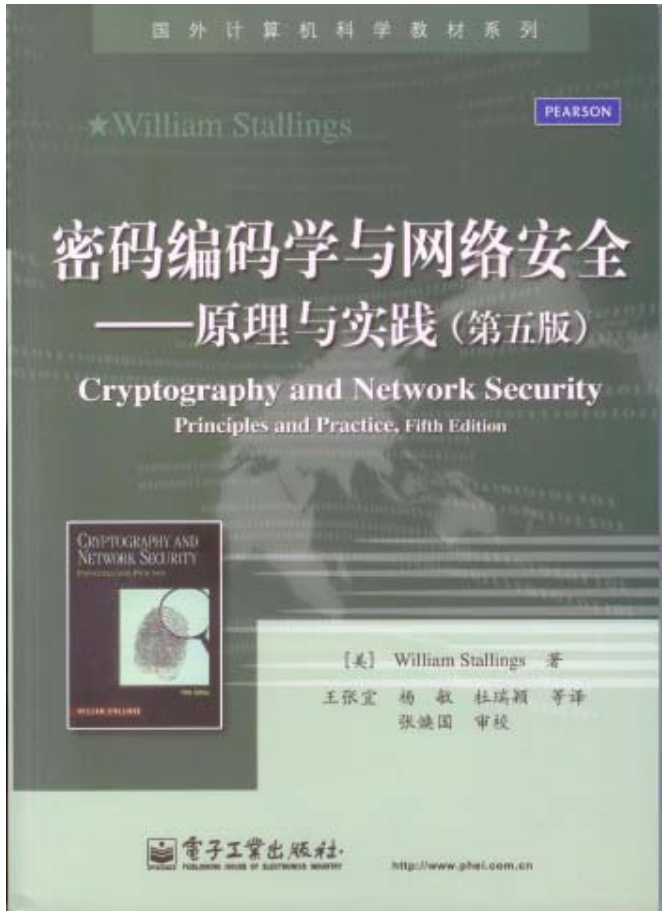
第十讲　公钥密码（2）
第十一讲　数字签名（1）
第十二讲　数字签名（2）
第十三讲　HASH函数
第十四讲　认证
第十五讲　密码协议
第十六讲　密钥管理（1）
第十七讲　密钥管理（2）
第十八讲　复习

教材与主要参考书

教材



参考书



一、武汉大学的信息安全学科

- 2001年武汉大学创建了全国第一个信息安全本科专业
- 2001-2003年武汉大学还建立了：
  信息安全硕士点、博士点、博士后产业基地
- 2007年1月“教育部高等学校信息安全类专业教学指导委员会”成立
- 2013年全国已有80多所高校建立了信息安全本科专业
- 2006年武汉大学信息安全专业获湖北省“品牌专业”
- 2007年武汉大学信息安全专业获“国家特色专业建设点”
- 2008年武汉大学建立“空天信息安全与可信计算“教育部重点实验室
- 2009年武汉大学的“密码学课程“被评为”国家精品课程”
- 武汉大学已成为我国信息安全科学研究和人才培养的重要基地

二、二十一世纪是信息的时代

1、二十一世纪是信息时代

- 人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。
- 信息产业超过钢铁、机械、石油、汽车、电力等传统产业，成为世界第一大产业。
- 信息和信息技术改变着人类的生活和工作方式。离开计算机、网络、电视和手机等电子信息设备，人们将无法生活和工作。
- 信息成为重要的战略资源。信息的获取、存储、传输、处理和安全保障能力成为综合国力和经济竞争力的重要组成部分。
- 信息安全事关国家安全，事关经济发展，事关社会稳定。

二、二十一世纪是信息的时代

2、信息技术与产业空前繁荣

- 信息社会正按摩尔定律、吉尔德定律、千倍定律高速发展。
- 比尔盖茨连续13年世界首富，08年退休，把自己的580亿美元资产全部捐献给以他命名的慈善基金会。
- 2011年6月美国Apple公司的资产世界第一，相当于165个国家GDP之和。

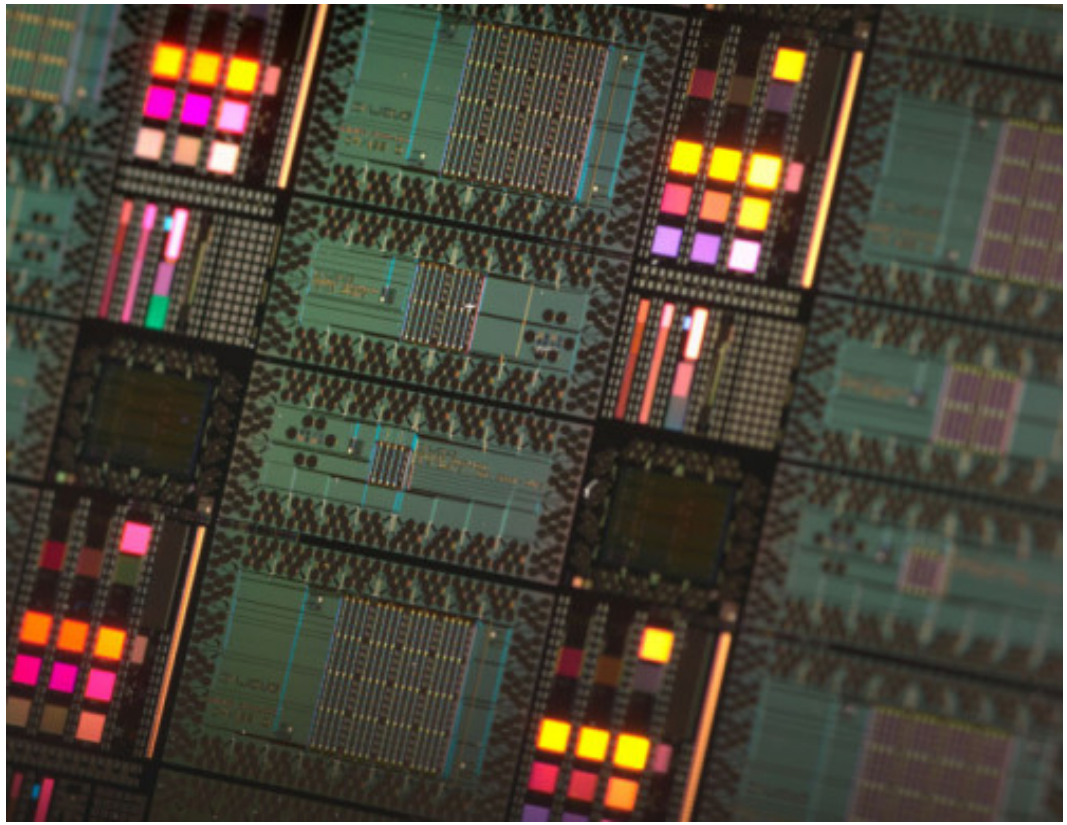
二、二十一世纪是信息的时代

3、新型计算机已经出现

①量子计算机：

- 加拿大的量子计算机：
  - 2007年2月加拿大的D-Wave System公司宣布研制出世界上第一台商用16量子位的量子计算机。
  - 2008年提高到48量子位。
  - 2011年5月30日，提高到128量子位，以1000万$一台出售。洛克希德马丁公司购买，用于F35战机等新式武器的研制。
  - 2013年初，又提高到512量子位，比3600台PC还要快。1500万$一台，谷歌公司购买。用于提高信息搜索速度。
- 加拿大的量子计算机的发展速度是惊人的，但它是专用型量子计算机，不是通用型量子计算机。

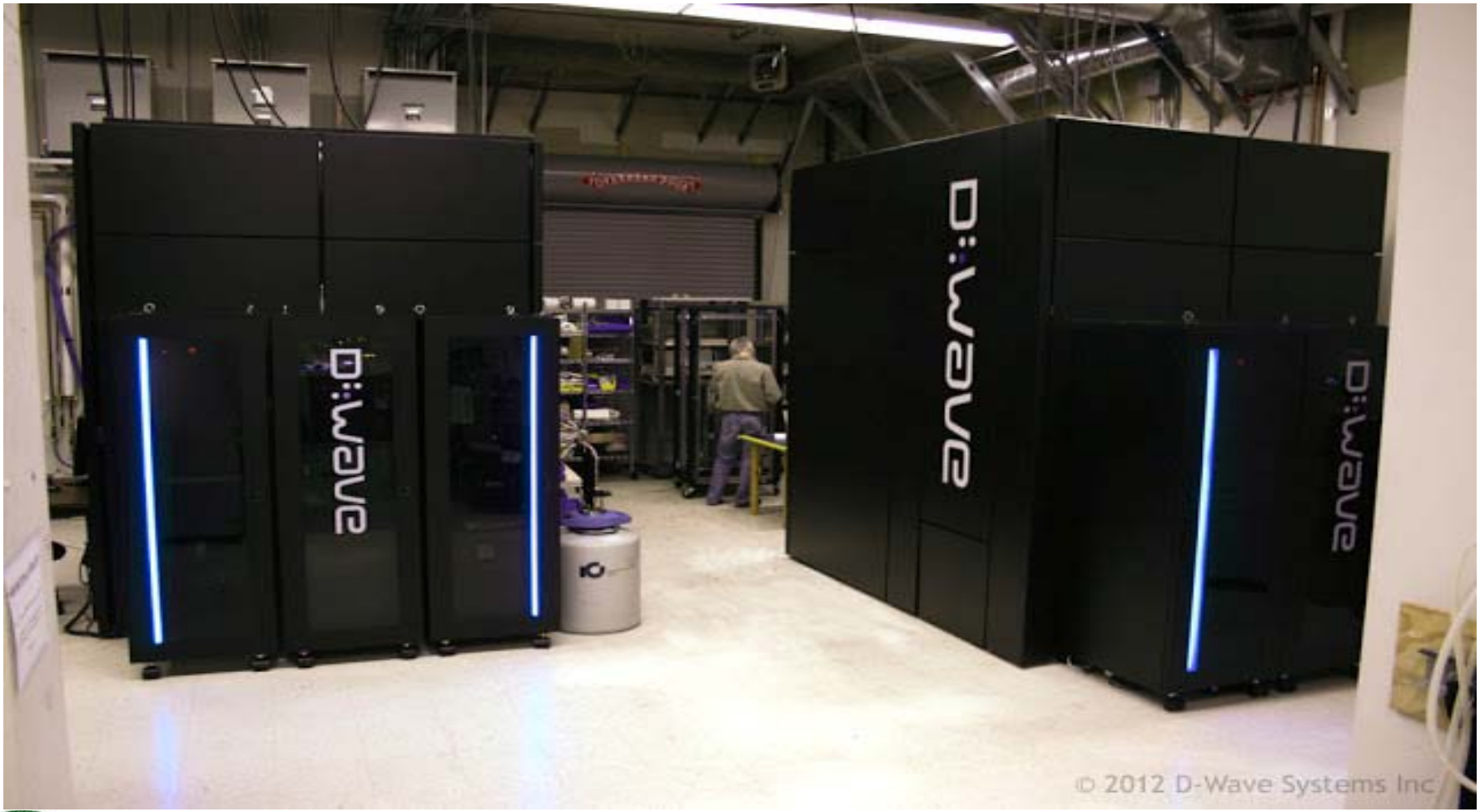
加拿大D-Wave System公司的量子计算机



128qbit量子计算机

处理器阵列

加拿大D-Wave System公司的量子计算机



512qbit量子计算机

二、二十一世纪是信息的时代

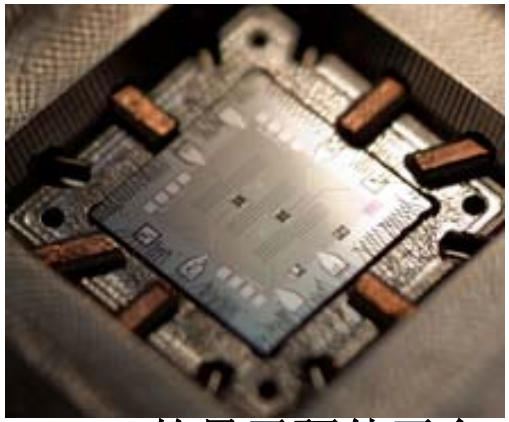
3、新型计算机已经出现

①量子计算机：

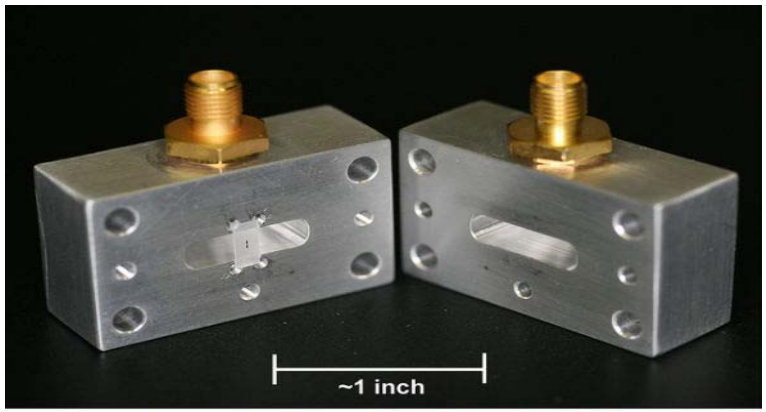
- 美国的量子计算机：
  - 美国政府和军方执行着5个量子计算研究计划，但具体进展却密而不宣。
  - 2011年9月，UCSB通过量子电路实现了冯诺依曼结构。
  - 2012年9月，UCSB宣布利用该硬件平台完成素数分解的Shor算法量子电路实验。
  - IBM找到了大规模提升量子计算机规模的一种关键技术。
- 如果量子计算机的规模进一步提高，将可攻破现有许多密码。
  - 1448位的量子计算机可以攻破256位的ECC
  - 2048位的量子计算机可以攻破1024位的RSA

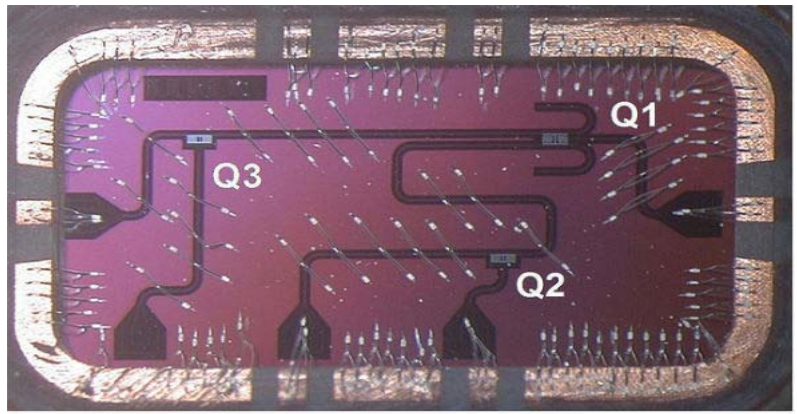
二、二十一世纪是信息的时代

美国的量子计算机技术



UCSB的量子硬件平台





IBM提升量子计算机规模的关键技术

二、二十一世纪是信息的时代

②DNA计算机

●1994年美国加州大学的L.Adleman提出DNA计算的思想，并在液体中进行实验。

●DNA计算的基本思想：

以DNA碱基序列为信息编码的载体，利用现代分子生物学技术，在试管内控制酶的作用下，进行DNA序列反应。反应前的DNA为输入，反应后的DNA为输出。

二、二十一世纪是信息的时代

② DNA计算机

- **DNA计算的特点：**
  - 高度并行：运算速度快，可达1.2×10^{18}次/s，比目前最快的电子计算机快得多。
  - 节能，能耗是目前超级计算机的$1/10^{18}$。
  - 信息存储密度高，每（纳米）^{3}1bit，而现在的存储介质每2^9（纳米）^{3}1bit。
- 2003年以色列研制出可人机交互DNA计算机
- L.Adleman用DNA计算机求解了一个24个未知数、100万种可能性的数学难题。
- 2012.2.8美国加州斯克里普斯研究院和以色列理工学院开发出一种生物计算机，可破译DNA芯片中的加密图像。

二、二十一世纪是信息的时代

4、我国成为世界信息大国

- 我国因特网用户量，居世界第1位。
- 我国手机拥有量，居世界第1位。
- 我国电话机拥有量，居世界第1位。
- 我国有线电视用户数，居世界第一。
- 大多数中低档电子产品，我国都居世界第一。

- 我国在高档和基础性IT技术方面尚落后：
  - 集成电路（CPU，专用电路）、高级电子仪器
  - 系统软件（OS，DB）、行业应用软件

三、信息安全形势严峻

由于信息是重要的战略资源，计算机系统集中管理着国家和企业的政治、军事、金融、商务等重要信息，因此计算机系统成为不法分子的主要攻击目标。又由于计算机系统本身的脆弱性和网络的开放性，使得信息安全成为世人关注的社会问题。当前，信息安全的形势是严峻的。

三、信息安全形势严峻

1、世界领导人的论述

●江泽民：大力推进信息化进程，高度重视信息网络安全。

●江泽民：积极发展，加强管理，趋利避害，为我所用，努力在全球信息网络化的发展中占据主动地位。

●克林顿：谁掌握了信息，谁就掌握了主动。

●普京：信息资源及其基础设施成为角逐世界领导地位的舞台。

三、信息安全形势严峻

1、世界领导人的论述

●胡锦涛：信息安全是个大问题，必须把信息安全问题放到致关重要的位置上，认真加以考虑和解决。

● 温加宝：面对多变的国际环境和互联网的广泛应用，我国信息安全问题日益突出。加入世界贸易组织、发展电子政务等，对信息的安全保障提出了新的、更高的要求。必须从经济发展、社会稳定、国家安全、公共利益的高度，充分认识信息安全的极端重要性。

三、信息安全形势严峻

2、反华势力的干扰

- 2002年在江泽民主席的767专机上查出27个窃听器。
- 2002年和2003年法轮功分子三次攻击鑫诺卫星，把信息对抗引入到空间领域。
- 2013美国棱镜计划曝光，美国中情局对中国等许多国家进行通信、邮件进行信息监控。

三、信息安全形势严峻

3、黑客入侵

●黑客入侵已经成为一种经常性、多发性的信息安全事件

●2000年2月7日起的一周内，黑客对美国的雅互等著名网站发动攻击，致使这些网战瘫痪，造成直接经济损失12亿美元。我国的163网战也陷入困境。

●2001年5月1日前后，发生了一场网上“ 中美黑客大战”，双方互相攻击对方的网站，双方都有很大损失。这场网上大战，给我们留下深刻的思考。

●2003年1月25日13时30分到19时30分的6个小时内，亚洲、北美和欧洲的NTERNET网络全部陷入瘫痪和半瘫痪状态。

三、信息安全形势严峻

4、利用计算机进行经济犯罪

- 利用计算机进行经济犯罪超过普通经济犯罪
  - 电信诈骗
  - 银行卡诈骗
- 我国的发案率每年高速度递增

5、计算机病毒

- 计算机病毒已超过 几万种，而且还在继续增加
- 病毒新趋势
  - 追求经济和政治利益
  - 团体作案

三、信息安全形势严峻

6、信息战

●信息技术的发展促进了军事革命，信息战、网络战成为重要作战形式。

- 95年美国提出信息作战的概念，并成立信息作战指导委员会
- 两次海湾战争中，美国都成功实施了信息战
- 2007年美国成立网络作战司令部
- 2011.5.16美国公布“网络空间国际战略”，7.14公布“网络空间作战战略”。提出“陆、海、空、天、网络”5维一体的美国国家安全概念，并认定攻击美国的网络视为对美国开战，美国可以使用一切战争手段反击
- 美国利用计算机病毒破坏伊朗铀离心机
- 伊朗利用电子技术捕获了美国的无人侦察机
- 12年1月5日美国宣布把战略重心放到亚太地区

三、信息安全形势严峻

7、我国基础信息技术与产品受控于国外

- **主要的集成电路芯片依赖进口**

  在集成电路中植入病毒、后门、窃听器是容易的。

- **操作系统等基础软件依赖国外**
  - 操作系统有漏洞
  - 数据库有漏洞
  - **BIOS**也有漏洞
  - 应用软件也有漏洞

三、信息安全形势严峻

8、确保我国信息安全是我国的国家战略

●党的十八大文件明确指出要“高度关注海洋、太空、网络空间安全”。

●国家领导人最近指出：“信息安全是最重要的国家安全”。

●因此，加快国家信息安全保障体系建设，确保我国的信息安全，已经成为我国的国家战略。

四、信息安全问题的技术根源

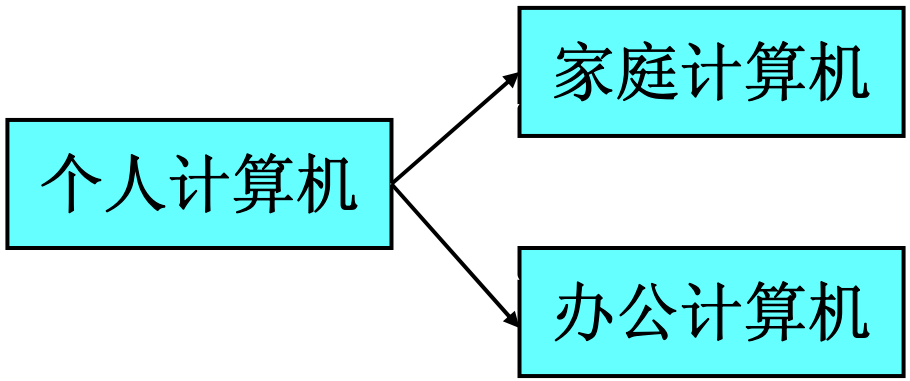
1、微机的安全结构过于简单

- 微机是个人计算机（**Personal Computer**）
- 去掉了许多成熟的安全机制
  - 存储器的隔离保护
  - 程序校验
- 程序的执行不经过认证
- 执行程序可被随意修改
- 系统区域的数据随意修改

} 病毒、蠕虫、木马

四、信息安全问题的技术根源

2、信息技术的发展使微机变成公用计算机



四、信息安全问题的技术根源

3、网络的发展使信息安全问题更加严重

- 网络连接突破了计算机机房的地理隔离
- 信息的I/O扩大到整个网络
- Internet网络缺少安全设计
- Internet网络无政府状态
- 网络协议存在安全缺陷和漏洞
- 正确的协议也可被利用进行攻击 DOS

四、信息安全问题的技术根源

4、软件存在安全缺陷

- 软件平均1000行代码就会存在一个安全漏洞
- 操作系统太庞大
- 操作系统不可能做到完全正确
- 缺陷造成的功能故障，往往可忽略
- 缺陷被攻击者利用所造成的安全后果，却不能忽略
- 数据库、应用软件都存在安全漏洞

五、信息安全学科概论

1、信息系统安全的概念

- 能源、材料、信息是支撑现代社会大厦的支柱！
  - 能源、材料是物质的、具体的
  - 信息是逻辑的、抽象的
  - 信息不能脱离信息系统而独立存在！
- 不能脱离信息系统孤立地谈论信息安全！
- 信息系统安全的立体视角，四个层面的安全：

  设备安全，数据安全，内容安全，行为安全

  中文词安全＝**Security + Safety**
  - **Security**是指阻止人为恶意地对安全的危害。
  - **Safety**是指阻止非人为对安全的危害，或人为但非恶意。

五、信息安全学科概论

①设备安全的概念

- 信息设备的安全是信息系统安全的首要问题
  - 设备的稳定性(Stability)

    设备在一定时间内不出故障的概率。
  - 设备的可靠性(Reliability)

    设备能在一个给定时间内正常执行任务的概率。
  - 设备的可用性(Availabity)

    设备随时可以正常使用的概率。
- 设备：硬设备，软设备

五、信息安全学科概论

②数据安全

- 采取措施确保数据免受未授权的泄露、篡改和毁坏。
  - ■数据的秘密性(Secrecy)

    数据不被未授权者知晓的属性
  - ■数据的完整性(Integrity)。

    数据是正确的、真实的、未被篡改的、无缺失的属性
  - ■数据的可用性(Availabity)

    数据是随时可以使用的属性
- 传统的信息安全主要指数据安全

五、信息安全学科概论

③内容安全

- 内容安全是信息安全在法律、政治、道德层次上的要求。
  - ■信息内容在政治上是健康的
  - ■信息内容符合我国法律法规
  - ■信息内容符合中华民族优良的道德规范

五、信息安全学科概论

④行为安全

- 行为安全从主体的行为考察是否能够确保信息安全。
- 符合哲学上实践是检验真理的唯一标准的原理。
  - 行为的秘密性：行为不能危害数据秘密性，需要时行为本身也是秘密的
  - 行为的完整性：行为不能危害数据完整性，行为的过程和目标是预期的
  - 行为的可控性：当行为的过程出现偏离预期时，能够发现、控制或纠正

五、信息安全学科概论

2、信息安全措施

- 信息安全措施＝{法律措施，教育措施，管理措施，技术措施，…}

注意：

- 决不能低估法律、教育、管理的作用，许多时候它们的作用大于技术。
- 信息安全界的行话：“三分技术，七分管理”
- 确保信息安全是一个系统工程，必须综合采取各种措施才能奏效。

五、信息安全学科概论

- 信息安全的技术措施

  信息安全技术措施＝{硬件系统安全、操作系统安全、密码技术、网络安全技术、软件安全技术、病毒防治技术，信息内容安全技术，信息隐藏技术，信息对抗技术，取证技术，容错技术，…}。

- 注意
  - 信息系统的硬件系统安全和操作系统安全是信息系统安全的基础，密码技术、网络安全技术等是关键技术。

五、信息安全学科概论

- 信息安全的管理措施
  - 信息安全管理措施既包括信息设备、机房的安全管理，又包括对人的安全管理，其中对人的管理是最主要的。
  - 行话：“三分技术，七分管理。”

- 信息安全的法律措施
  - 法律是武器。
  - 我国政府关于信息安全的各种法律法规。

五、信息安全学科概论

- 信息安全的教育措施
  - 对人的思想品德教育、安全意识教育、安全法律法规的教育等。
  - 国内外的计算机犯罪事件都是人的思想品德出问题造成的。

确保信息安全是一个系统工程必须综合采取各种措施才能奏效！

五、信息安全学科概论

3、信息安全学科内涵

- 信息安全学科是研究信息获取、信息存储、信息传输和信息处理领域中信息安全保障问题的一门新兴学科。
- 信息安全学科是计算机、电子、通信、数学、物理、生物、管理、法律和教育等学科交叉融合而形成的一门新型学科。它与这些学科既有紧密的联系，又有本质的不同。信息安全学科已经形成了自己的内涵、理论、技术和应用，并服务于信息社会，从而构成一个独立的学科。

五、信息安全学科概论

4、信息安全学科的研究方向与内容

①密码学

- 密码学由密码编码学和密码分析学组成，其中密码编码学主要研究对信息进行编码以实现信息隐蔽，而密码分析学主要研究通过密文获取对应的明文信息。密码学研究密码理论、密码算法、密码协议、密码技术和密码应用等。
  - 对称密码
  - 公钥密码
  - Hash函数
  - 密码协议
  - 新型密码：生物密码，量子密码等
  - 密码应用

五、信息安全学科概论

4、信息安全学科的研究方向与内容

②网络安全

- 网络安全的基本思想是在网络的各个层次和范围内采取防护措施，以便能对各种网络安全威胁进行检测和发现，并采取相应的响应措施，确保网络环境的信息安全。网络安全的研究网络安全威胁、网络安全理论、网络安全技术和网络安全应用等。
  - 通信安全
  - 协议安全
  - 网络防护
  - 入侵检测
  - 入侵响应
  - 可信网络

五、信息安全学科概论

4、信息安全学科的研究方向与内容

③信息系统安全

- 信息系统是信息的载体，是直接面对用户的服务系统。信息系统安全的特点是从系统级的整体上考虑安全威胁与防护。它研究信息系统的安全威胁、信息系统安全的理论、信息系统安全技术和应用。
  - 硬件系统安全
  - 软件系统安全
  - 访问控制
  - 可信计算
  - 信息系统安全测评认证
  - 信息系统安全等级保护

五、信息安全学科概论

4、信息安全学科的研究方向与内容

④信息内容安全

- 信息内容安全是信息安全在政治、法律、道德层次上的要求。我们要求信息内容是安全的，就是要求信息内容在政治上是健康的， 在法律上是符合国家法律法规的，在道德上是符合中华民族优良的道德规范的。
  - 信息内容的获取
  - 信息内容的分析与识别
  - 信息内容的管理和控制
  - 信息内容安全的法律保障

作 业 题

1、p7第2题。

2、 p7第5题。

谢　谢！