1. **信息安全问题的技术根源**
   1. 微机的安全结构过于简单：去掉了许多成熟的安全机制，如存储器的隔离保护 程序校验，导致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。
   2. 信息技术的发展使微机变成公用计算机。
   3. 网络的发展使微机变成网络中的一部分：
      1. 信息的I/O扩大到整个网络
      2. Internet网络缺少安全设计
      3. Internet网络无政府状态
      4. 网络协议存在安全缺陷和漏洞
      5. 正确的协议也可被利用进行攻击 DOS
   4. 操作系统存在安全缺陷
      1. 操作系统太庞大，且不可能做到完全正确
      2. 缺陷造成的功能故障，往往可忽略；但缺陷被攻击者利用所造成的安全后果，却不能忽略
2. **信息安全的基本概念**
   1. 计算机系统的安全服务功能：身份认证服务、访问控制服务、数据加密服务、数据完整性服务、不可否认服务、安全审计
   2. 信息系统安全的四个层面：
      1. 设备安全：**首要问题**，包括硬设备和软设备，三个侧面：稳定性(Stability)、可靠性(Reliability)、可用性(Availability)。
      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，三个侧面：秘密性(Secrecy)、数据的真实性 (Authenticity)、数据的完整性(Integrity)。信息安全采取的措施需要付出时间和空间的代价。
      3. 内容安全：在法律（合法合规）、政治（健康）、道德（符合中华民族道德规范）层次上的要求。
      4. 行为安全：**终极目的**，三个侧面：
         1. 私密性：行为不能危害数据秘密性；
         2. 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；
         3. 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。
   3. 信息安全措施：包括法律、教育、管理、技术（基础：硬件系统、操作系统；关键技术：密码、网络安全）措施。
3. **信息安全的理论与技术**
   1. 理论上信息安全是**不可判定**问题。不可判定是算法学概念，本质是人与人的斗争。
   2. 密码学的理论基础是**信息论**和**计算复杂性理论**。只能证明一个密码是不安全的，不能证明是安全的。理论上安全的密码是存在的，但任何可实用的密码都是可破译的。
   3. 系统结构安全、网络安全、操作系统安全等尚缺少完备的理论基础，因而缺少完善的方法和满意效果。
   4. 信息论呈现出局限性：
      1. 商农信息论的模型：点点通信模型；
      2. 网络、操作系统都不能用点点通信的模型描述；
      3. 信息论解决了信息传输和存储中的安全问题，没有涉及信息**处理**中的安全问题；
      4. 密码不能解决信息处理的安全问题，如病毒；