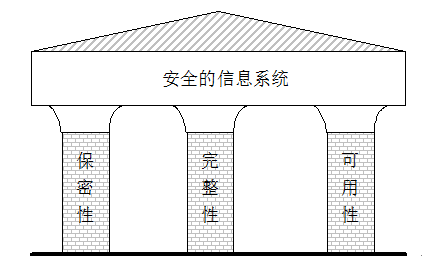
* **1. 网络信息面临哪些安全威胁？**
* **2. 信息安全的概念**
* **在英文中，与“信息安全”相关度最高的两个词汇是“Information Security”和“Cyber Security”。**
* **从词意本身来讲，“Information Security”的含义较广，包括一切与信息的产生、传递、储存、应用、内容等有关的安全问题。**
* **“Cyber Security”则更加明确，是指在网络空间中的安全，这是由于互联网在社会中的角色越来越重要，且信息安全事件通常都与互联网有着直接或间接的关系。**
* **因而，近年来在新闻报道、官方文件、学术论文和专著中“Cyber Security”的使用频率更高。**
* **本课研究的是网络空间（Cyberspace）中的信息安全。**
* **网络霸权** 
  + **本案例中的全球网络监控**
  + **美国坚决把持全球互联网的域名解析权**
  + **美国控制互联网根服务器**
  + **美国掌握着全球IP 地址的分配权**
  + **美国拥有世界上最大的、最主要的软件、硬件及互联网服务商**
  + **美国积极研制网络空间武器，强化在网络空间领域的霸主地位**
  + **美国将互联网当作对他国进行意识形态渗透的重要工具**
* **网络恐怖主义**
  + **如著名的恐怖组织“基地组织”以及近年活跃的极端恐怖组织ISIS，就非常善于利用网络，通过散布激进言论、散布谣言、散布血腥视频、攻击和破坏网络系统等方式造成社会轰动效应，增加对方（通常是国家）民众的恐惧心理，以达到破坏其社会稳定，甚至颠覆国家政权的目的。**
* **网络谣言和网络政治动员**
  + **所谓政治动员，是指在一定的社会环境与政治局势下，动员主体为实现特定的目的，利用互联网在网络虚拟空间有意图地传播针对性的信息，诱发意见倾向，获得人们的支持和认同，号召和鼓动网民在现实社会进行政治行动，从而扩大自身政治资源和政治行动能力的行为和过程。**
  + **当然，网络政治动员的作用是双面的，如果合理利用，也可以产生良好的正面效果。**
* **网络欺凌** 
  + **个人或群体利用网络的便捷性，通过计算机或手机等电子媒介，以电子邮件、文字、图片、视频等方式对他人所进行的谩骂、嘲讽、侮辱、威胁、骚扰等人身攻击，从而造成受害者精神和心理创伤。**
* **网络霸权**
* **网络恐怖主义**
* **网络谣言和网络政治动员**
* **网络欺凌**
* **网络攻击**
* **更具体地，根据信息流动过程来划分安全威胁的种类。**
* **设信息是从源地址流向目的地址，那么正常的信息流向如图所示。**
* **中断(Interruption)威胁：使得在用的信息系统毁坏或不能使用，即破坏可用性。**
* **攻击者可以从下列几个方面破坏信息系统的可用性：**
  + **使合法用户不能正常访问网络资源。**
  + **使有严格时间要求的服务不能及时得到响应。**
  + **摧毁系统。物理破坏网络系统和设备组件使网络不可用，或者破坏网络结构使之瘫痪等。如硬盘等硬件的毁坏，通信线路的切断，文件管理系统的瘫痪等。**
* **截获(Interception)威胁：是指一个非授权方介入系统，使得信息在传输中被丢失或泄露的攻击，它破坏了保密性。非授权方可以是一个人、一个程序或一台计算机。**
* **这种攻击主要包括：**
  + **利用电磁泄露或搭线窃听等方式可截获机密信息，通过对信息流向、流量、通信频度和长度等参数的分析，推测出有用信息，如用户口令、账号等。**
  + **非法复制程序或数据文件。**
* **篡改(Modification)威胁：以非法手段窃得对信息的管理权，通过未授权的创建、修改、删除和重放等操作而使信息的完整性受到破坏。**
* **这些攻击主要包括：**
  + **改变数据文件，如修改数据库中的某些值等。**
  + **替换某一段程序使之执行另外的功能，设置修改硬件。**
* **伪造(Fabrication)威胁中一个非授权方将伪造的客体插入系统中，破坏信息的可认证性。**
* **例如在网络通信系统中插入伪造的事务处理或者向数据库中添加记录。**
* **由于“信息”、“网络”、“安全”这几个概念的内涵与外延一直呈现不断扩大和变化的趋势，对于“信息安全”，目前还没有一个统一的定义。**
* **为此，本节接下来从对信息安全的感性认识、安全事件的发生机理、以及从安全的几大需求等多个角度来带领大家认识信息安全。**
* 如果我们的邮箱账户使用了强的口令（Password）是不是可以说邮箱就是安全的？
* 即使使用了强口令，但是用户对于口令保管不善，例如遭受欺骗而泄露，或是被偷窥
* 另一方面，由于网站服务商管理不善，明文保存用户口令并泄露用户口令，均会造成强口令失效。
* 如果我们的计算机从互联网完全断开是不是就可以确保我们计算机的安全？
* 即使我们的计算机完全与互联网断开，机器的硬件仍有被窃或是遭受自然灾害等破坏的风险
* 计算机中的数据仍有通过移动存储设备被传出的威胁。
* **可以说一个安全事件（Security Event）的发生是由于外在的威胁（Threat）和内部的脆弱点（Vulnerability）所决定的。**
* **在这里讨论信息安全的概念时，没有直接提及攻击（Attack），因为相对于表象具体的攻击，安全事件更具有一般性。本章案例中的“棱镜”计划的泄露算不上是斯诺登发起的一次网络攻击，它这次的机密信息的泄露的的确确算得上是一个安全事件。**
* **（1）威胁**
* **对信息系统的威胁是指：潜在的、对信息系统造成危害的因素。对信息系统安全的威胁是多方面的，目前还没有统一的方法对各种威胁加以区别和进行准确的分类，因为不同威胁的存在及其重要性是随环境的变化而变化的。**
* **这里将网络中的信息安全威胁分为三个层面：** 
  + **针对国家层面的国家行为的网络霸权威胁、非国家行为体的网络恐怖主义、网络谣言和网络社会动员；**
  + **针对组织和个人的网络攻击威胁；**
  + **针对个人的网络欺凌等威胁。**
* **（2）脆弱点**
* **信息系统中的脆弱点，有时又被称作脆弱性、弱点（Weaknesses）、安全漏洞（Holes）。**
* **物理安全、操作系统、应用软件、TCP/IP网络协议和人的因素等各个方面都存在已知或未知的脆弱点，它们为安全事件的发生提供了条件。**
* **（2）脆弱点**
* **1）物理**
* **计算机系统物理方面的安全主要表现为物理可存取、电磁泄露等方面的问题。此外，物理安全问题还包括设备的环境安全、位置安全、限制物理访问、物理环境安全和地域因素等。**
* **移动存储器小巧易携带、即插即用、容量大等特性实际上也是这类设备的脆弱性。**
* **例如机房安排的设备数量超过了空调的承载能力**
* **（2）脆弱点**
* **2）软件系统**
* **计算机软件可分为操作系统软件、应用平台软件（如数据库管理系统）和应用业务软件三类，以层次结构构成软件体系。**
* **可以说，任何一个软件系统都会因为程序员的一个疏忽、开发中的一个不规范等原因而存在漏洞。**
* **（2）脆弱点**
* **3）网络和通信协议**
* **TCP/IP协议栈在设计时，只考虑了互联互通和资源共享的问题，并未考虑也无法同时解决来自网络的大量安全问题。**
* **例如电子邮件没有认证和加密。**
* **（2）脆弱点**
* **4）人的脆弱点**
* **人是信息活动的主体，人的因素其实是影响信息安全问题的最主要因素，例如下面3种情况。**
  + **人为的无意失误。**
  + **人为的恶意攻击。**
  + **管理上的因素。**



* **（1）CIA安全需求模型**
* **1）保密性（Confidentiality）**
* **保密性是指确保信息资源仅被合法的实体（如用户、进程等）访问，使信息不泄漏给未授权的实体。**
* **这里所指的信息不但包括国家秘密，而且包括各种社会团体、企业组织的工作秘密及商业秘密，个人的秘密和个人隐私（如浏览习惯、购物习惯等）。**
* **（1）CIA安全需求模型**
* **1）保密性（Confidentiality）**
* **实现保密性的方法一般是通过对信息加密，或是对信息划分密级并为访问者分配访问权限，系统根据用户的身份权限控制对不同密级信息的访问。**
* **（1）CIA安全需求模型**
* **2）完整性（Integrity）**
* **完整性是指信息资源只能由授权方或以授权的方式修改，在存储或传输过程中不被偶然或蓄意地修改、伪造等破坏。**
* **不仅仅要考虑数据的完整性，还要考虑操作系统的逻辑正确性和可靠性，要实现保护机制的硬件和软件的逻辑完备性、数据结构和存储的一致性。**
* **（1）CIA安全需求模型**
* **3）可用性（Availability）**
* **可用性是指信息资源可被合法用户访问并按要求的特性使用而不遭拒绝服务。**
* **可用的对象包括：信息、服务、IT资源等。例如在网络环境下破坏网络和有关系统的正常运行就属于对可用性的攻击。**
* **为了实现可用性可以采取备份与灾难恢复、应急响应、系统容侵等许多安全措施。**
* **（2）其他安全需求**
* **不可抵赖性通常又称为不可否认性，是指信息的发送者无法否认已发出的信息或信息的部分内容，信息的接收者无法否认已经接收的信息或信息的部分内容。实现不可抵赖性的措施主要有：数字签名、可信第三方认证技术等。**
* **可认证性是指，保证信息使用者和信息服务者都是真实声称者，防止冒充和重演的攻击。**
* **（2）其他安全需求**
* **可控性是指，对信息和信息系统的认证授权和监控管理，确保某个实体（用户、进程等）身份的真实性，确保信息内容的安全和合法，确保系统状态可被授权方所控制。**
* **管理机构可以通过信息监控、审计、过滤等手段对通信活动、信息的内容及传播进行监管和控制。**
* **（2）其他安全需求**
* **可审查性是指，使用审计、监控、防抵赖等安全机制，使得使用者（包括合法用户、攻击者、破坏者、抵赖者）的行为有证可查，并能够对网络出现的安全问题提供调查依据和手段。**
* **审计是通过对网络上发生的各种访问情况记录日志，并对日志进行统计分析，是对资源使用情况进行事后分析的有效手段，也是发现和追踪事件的常用措施。**
* **审计的主要对象为用户、主机和节点，主要内容为访问的主体、客体、时间和成败情况等。**
* **（2）其他安全需求**
* **可存活性是指，计算机系统的这样一种能力：它能在面对各种攻击或错误的情况下继续提供核心的服务，而且能够及时地恢复全部的服务。**
* **这是一个新的融合计算机安全和业务风险管理的课题，它的焦点不仅是对抗计算机入侵者，还要保证在各种网络攻击的情况下业务目标得以实现，关键的业务功能得以保持。**
* **信息安全是特定对象的安全，也是特定过程的安全。**
* **从信息安全要保护的对象来看，包括信息基础设施、计算环境、边界和连接、信息内容以及信息的应用；**
* **从过程来看，信息要保护的是信息生产、存储、传输、处理、使用直至销毁的全过程。**
* **围绕构建信息安全体系结构的人、技术和管理三个关键要素展开。**
* **信息安全技术介绍七大方面：设备与环境安全、数据安全、身份与访问安全、系统软件安全、网络安全、应用软件安全、信息内容安全，涵盖了从硬件到软件，从主机到网络，从数据到内容等不同层次的安全问题及解决手段。**
* **此外，信息安全管理介绍信息安全管理体系和信息安全工程，涵盖了从规划、测评，到实施、评估等不同环节的安全手段。**

**数据安全要求：**

**确保数据的保密性、完整性、不可否认性和可认证性**

**基础是现代密码学。**

**通过加密将可读的信息变换成不可理解的乱码，从而起到保护信息的作用；**

**密码技术还能够提供完整性检验，即提供一种当某些信息被修改时可被用户检验出的机制；**

**基于密码体制的数字签名具有抗抵赖功能，可使人们遵守数字领域的承诺。**

* **1. 密码基本概念**
* **2. 数据保护：保密性、完整性、不可否认性、可认证性和存在性**
* **3. 数据保护：可用性与容灾备份**



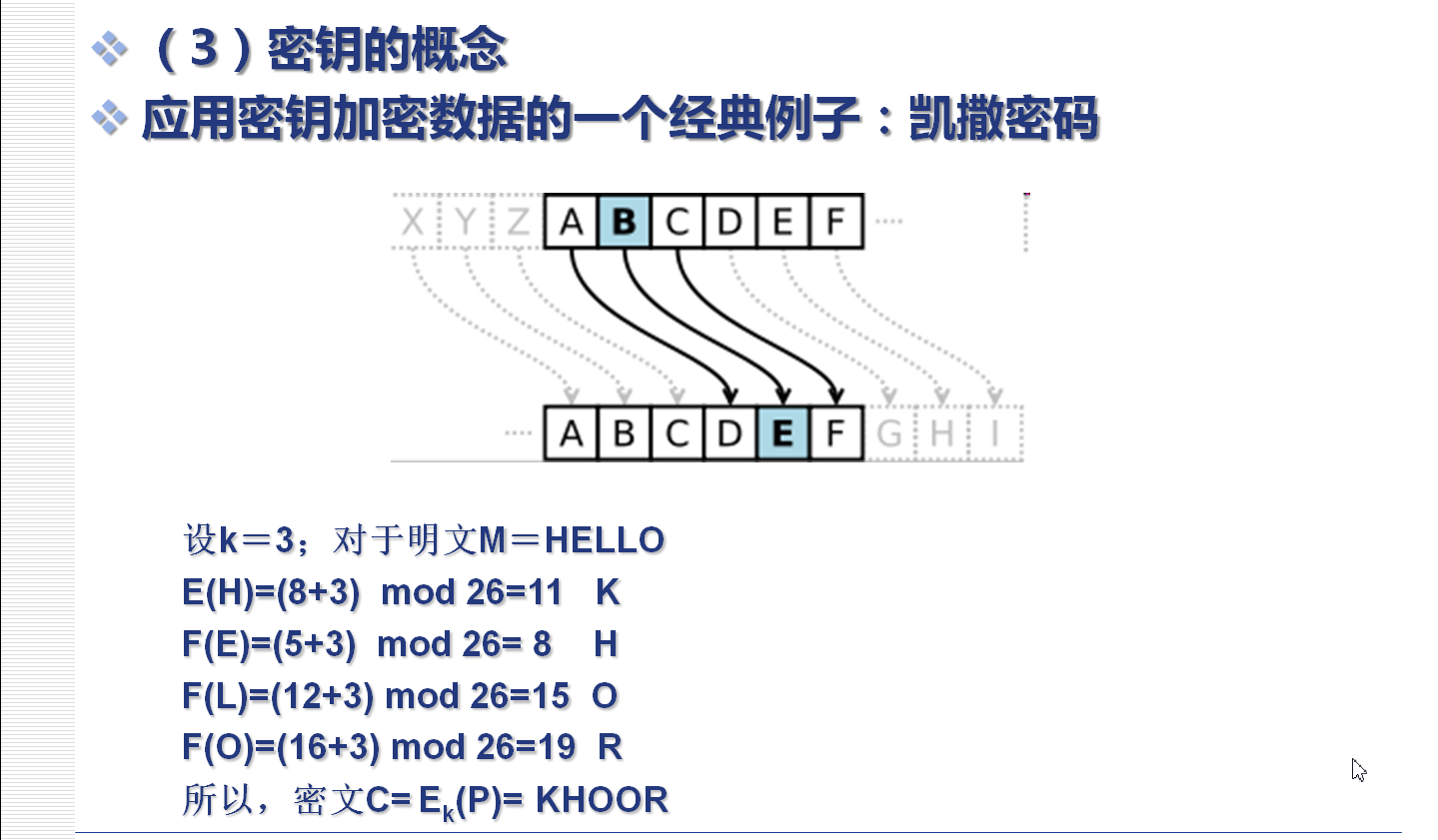
**保密通信中，通信双方要商定信息变换的方法，即加密和解密算法，使得攻击者很难破解，同时要求算法高速、高效和低成本。**

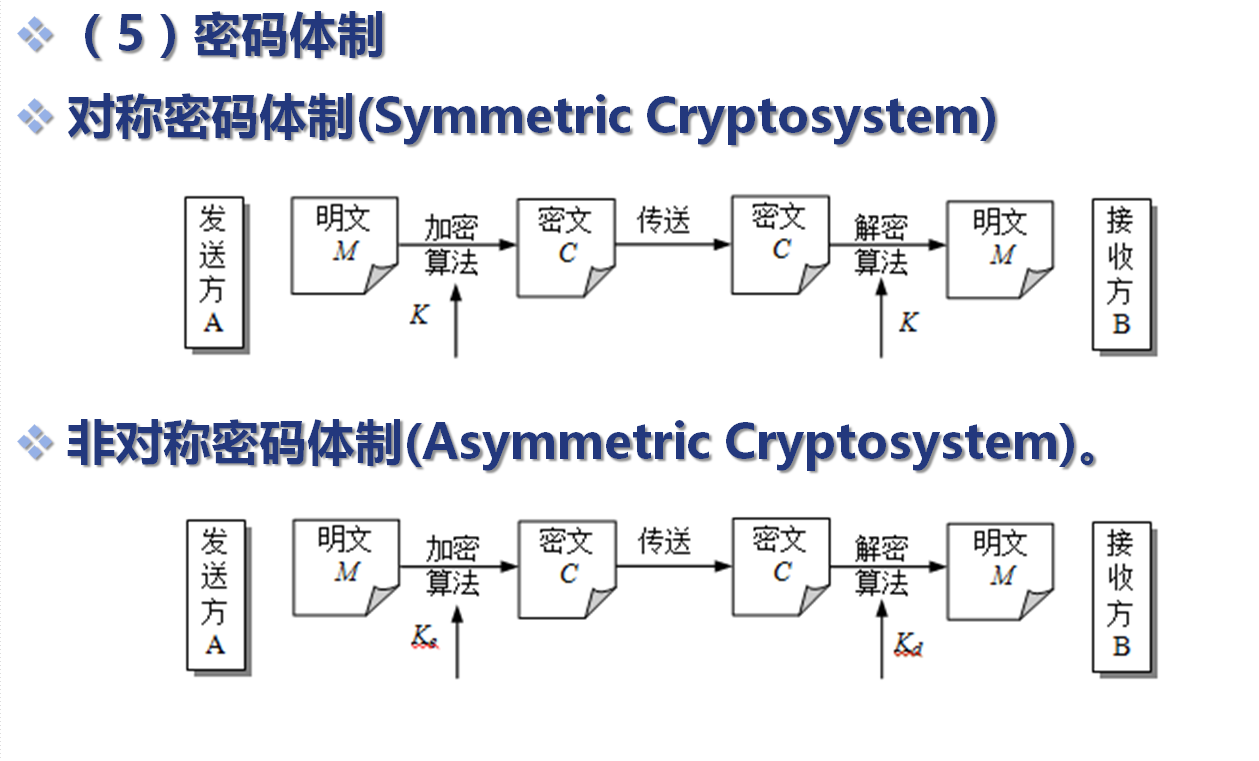
**研究把明文信息变换成不能破解或很难破解的密文的技术，称为密码编码学(Cryptography)**

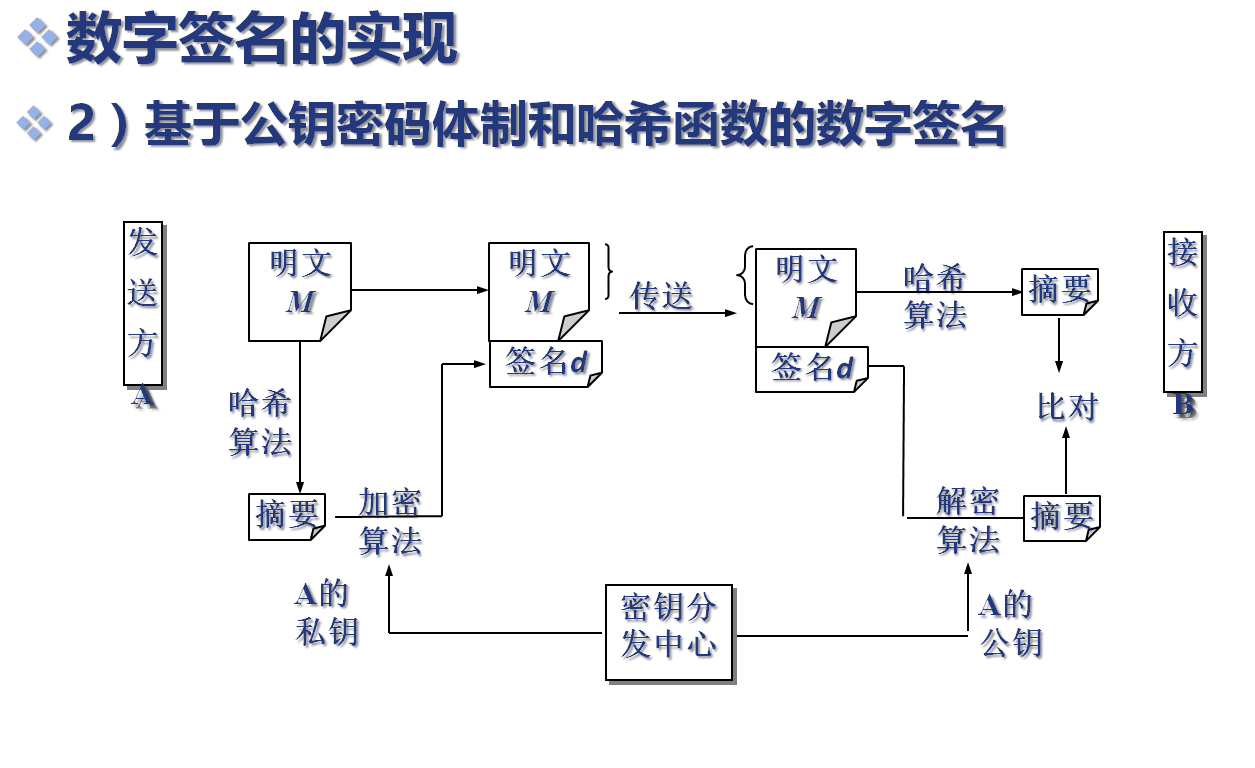
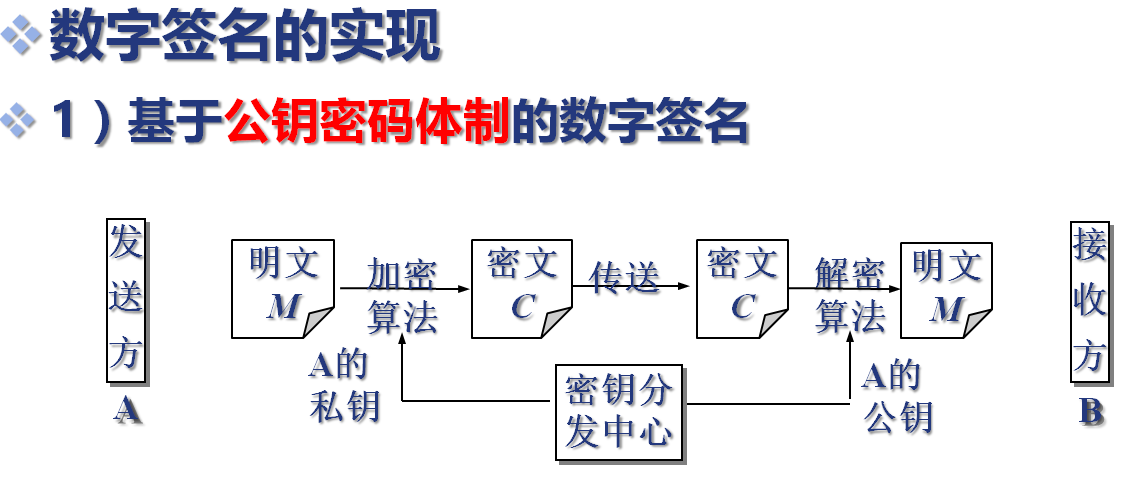
**攻击者对窃听或截取的密文会想方设法在有效时间内进行破解，以得到有用的明文信息。**

**研究分析破译密码，从密文推演出明文或相关内容的技术，称为密码分析学(Cryptanalysis)。**

* **1）保密通信基本过程**
* **现代密码技术已不仅仅限于保密通信的应用。**
* **现代密码技术及应用已经涵盖数据处理过程的各个环节，如数据加密、密码分析、数字签名、身份认证、秘密分享等。**
* **通过以密码学为核心的理论与技术来保证数据的机密性、完整性、不可否认性等多种安全属性。**
* **（2）密码的概念**
* **“密码(Cryptography)”与“口令（Password）”的区别。**
* **“密码”通常是密码算法的简称，它由加密算法和解密算法组成。**
* **一种古老的密码**
* **（3）密钥的概念**
* **什么是受限算法？**
* **如果算法的保密性是基于保持算法的秘密，就称为受限算法。**
* **受限算法的安全问题**
* **保密性已远远不够!**
* **密钥的作用**



* **（4）密码的安全性**
* **1）穷举攻击**
* **穷举攻击又称作蛮力（Brute Force）攻击，是指密码分析者用试遍所有密钥的方法来破译密码。**
* **例如，对于上面介绍的凯撒密码，攻击者就可以通过穷举密钥1~25来尝试破解。**
* **2）统计分析攻击**
* **统计分析攻击是指密码分析者通过分析密文的统计规律来破译密码。**
* **例如，对于上面的恺撒密码就可以通过分析密文字母和字母组的频率而破译。**
* **（4）密码的安全性**
* **2）统计分析攻击**
* **实际上，凯撒密码这种字母间的变换并没有将明文字母出现的频率掩藏起来，很容易利用频率分析法进行破解。**
* **所谓频率分析，就是基于某种语言中各个字符出现的频率不一样，表现出一定的统计规律，这种统计规律可能在密文中得以保存，从而通过一些推测和验证过程来实现密码的分析。**
* **对抗统计分析的方法**
* **1）混乱性（Confusion）。当明文中的字符变化时，截取者不能预知密文会有何变化，把这种特性称为混乱性。混乱性好的算法，其明文、密钥和密文之间有着复杂的函数关系。这样，截取者就要花很长时间才能确定明文、密钥和密文之间的关系，从而要花很长的时间才能破译密码。**
* **2）扩散性（Diffusion）。密码还应该把明文的信息扩展到整个密文中去，这样，明文的变化就可以影响到密文的很多部分，把这种特性称为扩散性。这是一种将明文中单一字母包含的信息散布到整个输出中去的特性。好的扩散性意味着截取者需要获得很多密文，才能去推测加密算法。**
* **3）数学分析攻击**
* **密码分析者针对加密算法的数学依据，通过数学求解的方法来破译密码。**
* **为了对抗这种数学分析攻击，应选用具有坚实数学基础和足够复杂的加密算法。**
* **4）社会工程攻击**
* **通过欺骗、威胁、勒索、行贿，或者折磨密钥拥有者，直到他给出密钥，这些社会工程学攻击也是一种破解密码的途径。**
* **信息隐藏技术是对付这种攻击的方法。**
* **小结**
* **影响密码安全性的基本因素包括：密码算法的复杂度、密钥机密性和密钥长度等。**
* **密码算法本身的复杂程度或保密强度取决于密码设计水平、破译技术等，它是密码系统安全性的保证。**
* **对于密钥的机密性，早在1883年柯克霍夫(Kerckhoff)在其名著《军事密码学》中就提出了一个原则：密码的安全不依赖于对加密系统或算法的保密，而依赖于密钥。这一原则已被后人广泛接受，称为柯克霍夫原则(Kerckhoffs’ Principle)。**
* **（5）密码体制**
* **密码体制，也称为密码系统，是指明文、密文、密钥以及实现加解密算法的一套软硬件机制。由于密码算法决定密码体制，有时将密码体制和密码算法不加区分。**
* **根据加密密钥(通常记为*Ke*)和解密密钥(通常记为*Kd*)的关系，密码体制可以分为**
  + **对称密码体制(Symmetric Cryptosystem)**
  + **非对称密码体制(Asymmetric Cryptosystem)。**
* 对称密码体制，也称单钥或私钥密码体制，其加密密钥和解密密钥相同或实质上等同（Ke=Kd），即由其中一个很容易推出另一个。图所示为对称密码体制模型。
* 非对称密码体制，也称公钥或双密钥密码体制，其加密密钥和解密密钥不同（这里不仅Ke≠Kd，在计算上Kd不能由Ke推出），这样将Ke公开也不会损害Kd的安全。非对称密码体制模型如图所示。
* 
* **（6）密钥管理**
* **由于密码技术都依赖于密钥，因此密钥的安全管理是密码技术应用中非常重要的环节。**
* **只有密钥安全，不容易被敌手得到或破获，才能保障实际通信或加密数据的安全。**
* **密钥管理方法因所使用的密码体制而异，但对密钥的管理通常包括：如何在不安全的环境中，为用户分发密钥信息，使得密钥能够安全、正确并有效地使用，以及在安全策略的指导下处理密钥自产生到最终销毁的整个生命周期，包括密钥的产生、存储、备份/恢复、装入、分配、保护、更新、泄漏、撤销、销毁等。**
* **（6）密钥管理**
* **密钥产生：** 
  + **首先要求在安全的环境下产生，可以通过某种密码协议或算法生成。**
  + **其次，必须考虑具体密码算法的限制，根据不同算法检测，以避免得到弱密钥。**
  + **再次，在确定要产生的密钥的长度时，应结合应用的实际安全需求，如要考虑加密数据的重要性、保密期限长短、破译者可能的计算能力等。**
* **（6）密钥管理**
* **密钥分配，也称密钥分发：** 
  + **将密钥安全地分发给需要的用户，一般地，在通信双方建立加密会话前，需要进行会话密钥的分配。**
* **密钥使用：** 
  + **应当根据不同需要使用不同的密钥，如身份认证使用公私钥对、临时的会话使用会话密钥。**
  + **在保密通信中，每次建立会话都需要双方协商或分配会话密钥，而不应当使用之前会话所使用的会话密钥，更不能永远使用同一个会话密钥。**
  + **甚至在有些保密通信系统中，同一次会话经过一定时间或一定数据量之后，会强制要求通信各方重新生成会话密钥。**
* **（6）密钥管理**
* **除安全存储外，密钥在分发或传输过程中，也需要加强安全保护。** 
  + **如密钥传输时，可以拆分成两部分，并委托给两个不同的人或机构来分别传输，通过使用其他密钥加密来保护。**
* **（6）密钥管理**
* **密钥要能被撤销。** 
  + **密钥撤销的原因包括与密钥有关的系统被迁移，怀疑一个特定密钥已泄漏并受到非法使用的威胁，或密钥的使用目的被改变，等等。**
  + **一个密钥停用后可能还要保持一段时间，如用密钥加密的内容仍需保密一段时间，所以密钥的机密性要保持到所保护的信息不再需要保密为止。**
* **1. 密码基本概念** 
  + **1）密码与保密通信**
  + **2）密码的概念**
  + **3）密钥的概念**
  + **4）密码的安全性**
  + **5）密码体制**
  + **6）密钥管理**
* **加密算法**
* **常用的非对称密码算法：** 
  + **RSA**
  + **ElGamal**
  + **椭圆曲线密码**
* **加密算法**
* **对称、非对称密码算法使用场合：** 
  + **使用同样硬件实现，DES比RSA快大约1000倍。**
  + **在一些智能卡应用中也采用了RSA算法，速度都比较慢。**
  + **软件实现方法的速度要更慢一些，这与计算机的处理能力和速度有关。同样使用软件实现，DES比RSA快大约100倍。**
  + **在实际应用中，RSA算法很少用于加密大块的数据，通常采用混合密码系统。**
  + **首先使用RSA传送会话密钥（对称），然后采用该对称密钥加密数据。**
* **什么是数据的完整性？** 
  + **数据在存储、传输和处理中可能遭受未授权、未预期或无意的修改，这就破坏了数据的完整性。**
* **如何确保数据的完整性** 
  + **除了事前的访问控制，还可以通过事后的完整性检测。**
  + **本讲将介绍哈希函数，以及利用哈希函数进行消息的完整性检测。**
* **哈希函数的概念** 
  + **哈希（Hash）函数又称为散列函数、消息摘要（Message Digest）函数、杂凑函数。**
  + **哈希函数可以把任意长度的输入转换成固定长度的输出。**
  + **它是一种单向密码体制，即从一个明文到密文的不可逆映射，只有加密过程，没有解密过程。**
  + **与对称密码算法和公钥密码算法不同，哈希函数没有密钥。**
* **哈希函数的特点** 
  + **它能处理任意大小的信息，并将其摘要生成固定大小的数据块，对同一个源数据反复执行哈希函数总是得到同样的结果。**
  + **它是不可预见的。产生的数据块的大小与原始信息的大小没有任何联系，同时源数据和产生的数据块看起来没有明显关系，但源数据的一个微小变化都会对数据块产生很大的影响。**
  + **它是完全不可逆的。即哈希函数是单向的，从源数据很容易计算其散列值，没有办法通过生成的散列值恢复源数据。**
  + **它是抗碰撞的。即寻找两个输入得到相同的输出值在计算上不可行。**
* **哈希函数的应用** 
  + **2）消息认证**
  + **3）数字签名**
  + **4）保护用户口令**
    - **将用户口令的哈希值存储在数据库中，进行口令验证时只要比对哈希值即可。**
* **常用哈希函数** 
  + **MD5**
  + **SHA：SHA-1、SHA-2、SHA-3**
* **确保信息的不可否认性，就是要确保信息的发送者无法否认已发出的信息或信息的部分内容，信息的接收者无法否认已经接收的信息或信息的部分内容。**
* **确保信息的可认证性，就是要确保信息的发送者和接收者的真实身份，防止冒充和重放。**
* **实现不可否认性和可认证性的措施主要有：数字签名，可信第三方认证技术等。本讲将介绍数字签名相关的技术和方法。**
* **数字签名的概念**
  + **在传统的以书面文件为基础的日常事务处理中，通常采用书面签名的形式，如手写签名、印章、手印等，来确保当事人的身份真实和不可否认。**
  + **这样的书面签名具有一定的法律意义。在以计算机为基础的数字信息处理过程中，就应当采用电子形式的签名，即数字签名（Digital Signatures）。**
  + **数字签名是一种以电子形式存在于数据信息之中的，或作为附件，或逻辑上与之有关联的数据，可用于辨别签署人真实身份，并标明签署人对数据信息内容认可的技术。**
* **数字签名的特性** 
  + **不可否认：签署人不能否认自己的签名。**
  + **不可伪造：任何人不能伪造数字签名。**
  + **可认证：签名接收者可以验证签名的真伪，也可以通过第三方仲裁来解决争议和纠纷。签名接收者还可通过验证签名，确保信息未被篡改。**



* **数字签名算法**
* **目前主要采用基于公钥密码体制的数字签名，包括普通数字签名和特殊数字签名。** 
  + **普通数字签名算法有RSA、ElGamal、椭圆曲线数字签名算法等。**
  + **特殊数字签名有盲签名、代理签名、群签名等。**
* **信息隐藏的概念** 
  + **信息隐藏(Information Hiding)，是指将机密信息秘密隐藏于另一公开的信息（通常为称为载体）中，然后将其通过公开通道来传递。**
* **信息隐藏与加密的区别** 
  + **利用密码技术可以将机密信息变换成不可识别的密文，信息经过加密后容易引起攻击者的好奇和注意，诱使其怀着强烈的好奇心和成就感去破解密码。**
  + **但对信息隐藏而言，攻击者难以从公开信息中判断其中是否存在机密信息，从而保证机密信息的安全。**
  + **简单地说，加密保护的是信息内容本身，而信息隐藏则掩盖它们的存在。**
* **信息隐藏的原理** 
  + **人的生理学弱点。人眼的色彩感觉和亮度适应性缺陷、人耳的相位感知缺陷都为信息隐藏在图片、音频或视频等文件中提供了可能。**
  + **载体中存在冗余。例如多媒体信息本身存在很大的冗余性，网络数据包中存在冗余位。**
  + **因此，可以将机密信息进行加密后隐藏在一幅普通的图片（音频、视频、文档或数据包）中发送，这样攻击者不易对普通图片产生兴趣，而且由于经过加密，即使被截获，也很难破解其中的内容。**
  + **图片文件中隐藏信息的原理（LSB算法）**
  + **图像的能量集中在高几层位平面，图像对高几层的修改比较敏感。**
  + **图像的最低位平面甚至是最低的几层位平面几乎不含有信息量，对修改不敏感。**
* **可以用待隐藏信息去替换原始载体最低位平面或最低几层位平面，从而实现信息隐藏，又不会使载体发生视觉上的可察觉性改变信息隐藏的载体** 
  + **信息隐藏的载体除了上述的图像文件，还可以是：** 
    - **音频**
    - **视频**
    - **文本**
    - **数据库**
    - **文件系统**
    - **硬盘**
    - **可执行代码**
    - **网络数据包**
    - **……**
* **常用文档面临安全问题** 
  + **非授权访问，即未经文档的所有人同意，查看、修改、处理文档；**
  + **篡改，文档的内容被非授权修改；**
  + **伪造和否认，伪造和否认文档的内容；**
  + **意外损坏。**
* **常用文档安全防护：口令认证、修改权限保护**
* **不过，上述密码（口令）的设置对于文档的保护能力很弱，因为现在网上能够很容易找到破解这些密码（口令）的软件。这些软件本是为用户忘记了密码（口令）而帮助他们恢复的，然而可以恢复自己文档的密码，当然也可以恢复别人的密码了，不过这就不能算是恢复了，这些软件实际上成为了破解工具。**
* **常用文档安全防护：文档加密、隐藏保护**
* **修改文档的属性为“隐藏”，当然这需要在“文件夹选项”→“查看”页框中设置“隐藏文件和文件夹”。**
* **直接修改文件名的扩展名，如将doc的扩展名改成bmp，双击后将在绘图中打开该文件，然而无法正常显示该Word文件内容，准确地说，这是起到伪装的作用。**
* **使用信息隐藏工具常用文档安全防护：文档完整性检测和数字签名**
* **可以下载完整性检测工具，为文档计算哈希值，在传送文档时同时提供该文档的哈希值，以进行完整性检测。**
* **一些软件还提供了数字签名功能，例如Adobe Acrobat制作pdf文档的软件中，提供了为文档进行签名的功能。**
* **常用文档安全防护：PGP综合安全防护**
* **OpenPGP(RFC 4880)是世界上最广泛使用的电子邮件数字签名/加密标准，它源于PGP，定义了对信息的加密解密、签名、公钥私钥和数字证书等格式，通过对信息的加密、签名，以及编码变换等操作对信息提供安全保密服务。**
* **身份认证分为两个过程：标识与鉴别。** 
  + **标识（Identification）就是系统要标识实体的身份，并为每个实体取一个系统可以识别的内部名称——标识符ID。**
  + **识别实体真实身份的过程称为鉴别（Authentication），也有称作认证或验证。**
* **户名或账户就可以作为身份标识。为了对实体身份的正确性进行验证，实体往往还需要提供进一步的凭证，例如密码（口令）、令牌或是生物特征。**
* **系统会将实体提供的账号和凭证这两类身份信息与先前已存储的该实体的身份信息进行比较，如果相匹配，那么实体就通过了身份鉴别。**
* **创建和发布的身份信息必须具有3个特性：**
* **1）唯一性。标识符必须是唯一的且不能被伪造，防止一个实体冒充另一个实体。不同的计算机系统、不同的应用中，可以使用不同的方式来标识实体的身份：可以是一个唯一的字符串，可以是一张数字证书（类似于现实生活中的居民身份证），也可以是主机IP地址或MAC地址（Media Access Control，媒介访问控制）。**
* **例如：** 
  + **Windows系统的登录用户名和口令标识了一个用户的身份；**
  + **校园网用户登录学校图书馆资源时根据用户的IP地址确认用户主机的合法身份等。**
* **创建和发布的身份信息必须具有3个特性：**
* **2）非描述性。任何身份的标识都不能表明账户的目的，例如Administrator这样的身份标识对于攻击者太具有诱惑力了。**
* **3）权威签发。有的身份标识，如数字证书应当由权威机构颁发，以便对标识进行验真，或在出现争执时提供仲裁。**
* **如何提高口令质量？**
* **对于用户** 
  + **增大口令空间。**
  + **选用无规律的口令**
  + **多个口令**
  + **用工具生成口令**
* **对于网站** 
  + **登录时间限制。**
  + **登录次数限制。**
  + **尽量减少会话透露的信息。**
  + **增加认证的信息量。**
* 除因用户管理不善以及认证端数据库遭受攻击被拖库而泄露口令外，口令在传输的过程中也面临着被截获的威胁。
* 尽管引入散列函数的认证方案可以起到保密作用，但是攻击者可以监听用户计算机与服务器之间涉及登录请求/响应的通信，并截获用户名和口令散列值。攻击者可以构造一个口令字典，其中包括尽可能多的猜测的口令，计算它们的散列值并与截获的散列值比对；利用这样的“字典攻击”，攻击者能以很高的概率找到用户的口令。
* 此外，利用截获的散列值，攻击者可以在新的登录请求中将其提交到同一服务器，服务器不能区分这个登录请求是来自合法用户还是攻击者，这种攻击方式称为字典攻击。
* 原因：静态口令，登录信息不变。