密 码 学

（第一讲）

密码学的基本概念

张焕国

武汉大学计算机学院

目　录

目　录

一、信息安全学科概论

1、信息安全学科建设

- *2001年经教育部批准武汉大学创建了全国第一个信息安全本科专业；*
- *2007年全国信息安全本科专业已达70多所高校；*
- *2003年经国务院学位办批准武汉大学建立：*

  信息安全硕士点； 博士点；博士后流动站
- *2007年1月成立国家信息安全教指委*
- *2006年武汉大学信息安全专业获湖北省“品牌专业”*
- *武汉大学成为我国信息安全科学研究和人才培养的重要基地。*

一、信息安全学科概论

2、信息安全学科特点

- *信息安全学科是交叉学科：计算机、通信、数学、物理、生物、管理、法律等；*
- *具有理论与实际相结合的特点；*
- *信息安全技术强调整体性、系统性、底层性；*
- *对信息安全来说，法律、管理、教育的作用很大，必须高度重视。*
- *人才是关键，人的综合素质是关键的关键！*

一、信息安全学科概论

3、武汉大学的办专业思路

以学信息安全为主，兼学计算机、通信，同时加强数学、物理、法律等基础，掌握信息安全的基本理论与技能，培养良好的品德素质。

二、信息安全的基本概念

1、信息安全事关国家安全

信息成为社会发展的重要战略资源，信息技术改变着人们的生活和工作方式。信息产业成为新的经济增长点。社会的信息化已成为当今世界发展的潮流。

信息获取、处理和安全保障能力成为综合国力的重要组成部分。

信息安全事关国家安全，事关社会稳定。

二、信息安全的基本概念

2、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三根支柱。

信息是逻辑的、抽象的，不能脱离系统而独立存在！

① 信息系统安全包括四个层面

信息系统安全＝设备安全＋数据安全＋内容安全＋行为安全

简称信息系统安全为信息安全！

② 中文词安全＝Security＋ Safety

- 中文安全的含义等于英文Security 加上Safety的含义。
- Security是指阻止人为的对安全的危害。
- Safety是指阻止非人为的对安全的危害。

二、信息安全的基本概念

③信息系统设备安全的概念

- 信息系统设备的安全是信息系统安全的首要问题和基础之一。
- 三个侧面：*设备的稳定性(Stability)，设备的可靠性(Reliability)，设备的可用性(Availabity)*。
- 设备：*硬设备，软设备*

二、信息安全的基本概念

④数据安全的概念

IBM公司的定义：*采取措施确保数据免受未授权的泄露、篡改和毁坏。*

- 说明：这个定义明确了信息安全的三个侧面：数据的秘密性(Secrecy)，数据的真实性(Authenticity)，数据的完整性(Integrity)。
- 这个定义还说明了，为了信息安全必须采取措施，必须付出代价，代价就是资源（时间和空间）。

二、信息安全的基本概念

⑤内容安全的概念

- 内容安全是信息安全在法律、政治、道德层次上的要求。
  - *政治上健康*
  - *符合国家法律、法规*
  - *符合中华民族道德规范*

二、信息安全的基本概念

⑥行为安全的概念

- 行为安全是信息安全的终极目的。
  - *符合哲学上，实践是检验真理的唯一标准的原理。*
  - *从过去的仅看身份，发展为既看身份更看行为。*
  - *三个侧面：*

行为的秘密性；

行为的完整性

行为的可控性

二、信息安全的基本概念

3、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。*

①*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、通信安全、网络安全、数据库安全、病毒防治技术，防电磁辐射技术，信息隐藏技术，数字资源保护技术，电子对抗技术，…}。

注意：硬件结构的安全和操作系统安全是基础，密码、网络安全等是关键技术。

二、信息安全的基本概念

②*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。

目前，计算机网络系统安全的最大威胁之一是缺少有效的计算机网络安全监管。

③*信息安全的法律措施*

信息安全措施包括各级政府关于信息安全的各种法律、法规。

商用密码管理条例；

计算机安全管理条例；

因特网安全管理条例等。

二、信息安全的基本概念

④ *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。

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。

二、信息安全的基本概念

4、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。*

三、密码学的基本概念

- *密码技术是一门古老的技术。*
- *世界各国都视密码为武器。*
- *战争的刺激和科学技术的发展推动了密码学的发展。*
- *信息技术的发展和广泛应用为密码学开辟了广阔的天地。*

三、密码学的基本概念

我国的密码分级：

①核心密码：

用于保护党、政、军的核心机密。

②普通密码：

用于保护国家和事企业单位的低于核心机密而高于商用的机密信息。

③商用密码：

用于保护国家和事企业单位的非机密的敏感信息。

④个人密码：

用于保护个人的隐私信息。

前三种密码均由国家密码管理局统一管理！

三、密码学的基本概念

我国商用密码政策：

①**统一领导：**

国家密码管理局统一领导。

②**集中管理：**

国家密码管理局办公室集中管理。

③**定点研制：**

只允许定点单位进行研制。

④**专控经营：**

经许可的单位才能经营。

⑤**满足使用：**

国内各单位都可申请使用。

三、密码学的基本概念

1、密码的基本思想

- *伪装信息，使未授权者不能理解它的真实含义。*
- *所谓伪装就是对信息进行一组可逆的数学变换。*

伪装前的原始信息称为明文，伪装后的信息称为密文，伪装的过程称为加密。去掉伪装还原明文的过程成为解密。加密在加密密钥的控制下进行。解密在解密密钥的控制下进行。用于加密的一组数学变换称为加密算法。用于解密的一组数学变换称为解密算法。

三、密码学的基本概念

2、密码体制(Cryptosystem)的构成

密码体制由以下五部分组成：

①明文空间M：全体明文的集合

②密文空间C：全体密文的集合

③密钥空间K：全体密钥的集合，$K=<K_e, K_d>$

④加密算法E：一族由M→C的加密变换

⑤解密算法D：一族由C→M的解密变换。解密变换是加密变换的逆。

三、密码学的基本概念

对于一个确定的密钥，加密算法将确定出一个具体的加密变换，解密算法将确定出一个具体的解密变换，而且解密变换就是加密变换的逆变换。

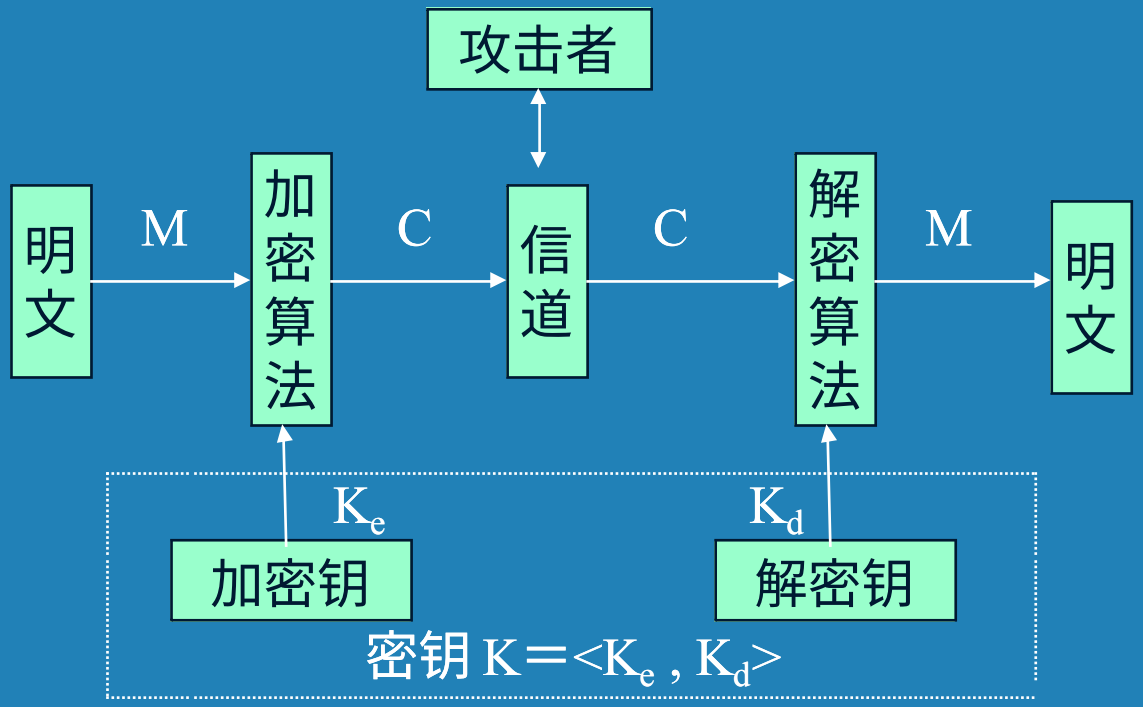
对于明文空间的每一个明文M，加密算法E在密钥K_e的控制下将明文M加密成密文C：

$$C = E(M, K_e)$$

而解密算法D在密钥K_d的控制下将密文解出同一明文M。

$$M = D(C, K_d) = D(E(M, K_e), K_d)$$

三、密码学的基本概念



三、密码学的基本概念

3、密码体制的分类

从加密钥与解密钥是否相等划分：

(1) 传统密码：

$$K_e = K_d$$

(2) 公开密钥密码：

$K_e \neq K_d$，且由K_e不能计算出K_d；

三、密码学的基本概念

从密钥的使用方式划分：

(1)序列密码：

①明文、密文、密钥以位（字符）为单位加解密；

②核心密码的主流；

(2)分组密码：

①明文、密文、密钥以分组为单位加解密；

②商用密码的主流：

三、密码学的基本概念

典型密码：

①传统密码：分组：DES IDEA EES AES

SMS4

序列：RC4

②公开密钥密码： RSA ELGamal ECC

二、密码学的基本概念

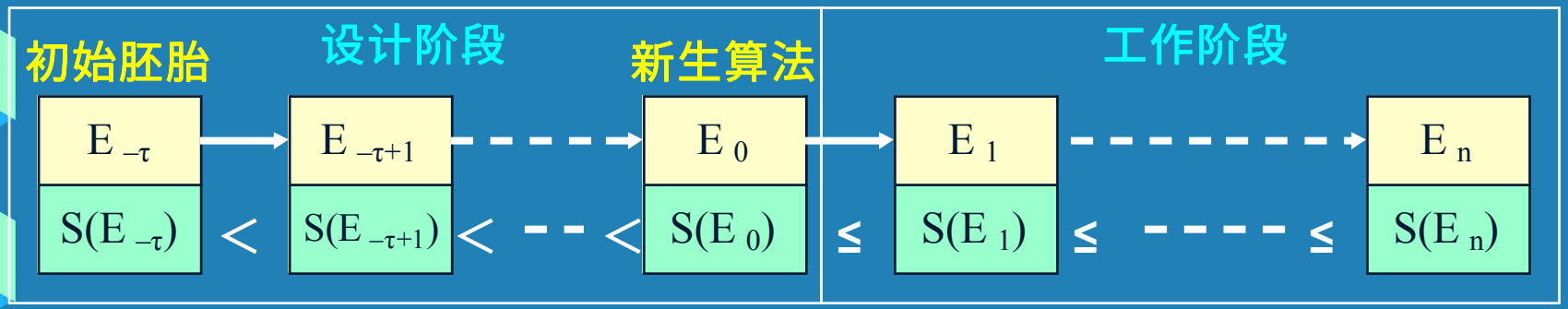
新型密码：

- *演化密码*

  ①密码算法不断演化变化，越来越强的密码。

  ②密码设计自动化的一种方法。

  ③借鉴生物进化，将密码学与演化计算结合



二、密码学的基本概念

新型密码：

- *量子密码*

  ①在唯密文攻击下绝对安全的密码。

  ②逐步走向实用。

  ③2007年我国宣布，国际上首个量子密码通信网络由我国科学家在北京测试运行成功。这是迄今为止国际公开报道的唯一无中转、可同时、任意互通的量子密码通信网络，标志着量子保密通信技术从点对点方式向网络化迈出了关键一步。

二、密码学的基本概念

新型密码：

- *DNA密码*
  - *DNA密码基于生物学中的某种困难问题。*
  - *由于DNA密码的安全不依赖于计算困难问题，所以不管未来的电子计算机、量子计算机和DNA计算机具有多么强大的计算能力，DNA密码对于它们的计算攻击都是免疫的。*

三、密码学的基本概念

4、密码学的组成

①研究密码编制的科学称为密码编制学(Cryptography)，

②研究密码破译的科学称为密码分析学(Cryptanalysis)，

③而密码编制学和密码分析学共同组成密码学(Cryptology)。

三、密码学的基本概念

5、密码分析

①如果能够根据密文系统地确定出明文或密钥，或者能够根据明文-密文对系统地确定出密钥，则我们说这个密码是可破译的。

②一个密码，如果无论密码分析者截获了多少密文和用什么方法进行攻击都不能被攻破，则称为是绝对不可破译的。

③绝对不可破译的密码学在理论上是存在的。

“一次一密”

三、密码学的基本概念

1）穷举攻击　密码分析者采用依次试遍所有可能的密钥对所获密文进行解密，直至得到正确的明文；或者依次用一个确定的密钥对所有可能的明文进行加密，直至得到所获得的密文。

显然，理论上，对于任何实用密码只要有足够的资源，都可以用穷举攻击将其改破。

三、密码学的基本概念

1）穷举攻击　实例

1997年美国一个密码分析小组宣布：1万多人参加，通过INTERNET网络，利用数万台微机，历时4个多月，通过穷举攻破了DES的一个密文。

美国现在已有DES穷举机，多CPU并行处理，24小时穷举出一个密钥。

三、密码学的基本概念

2)*统计分析攻击*　*所谓统计分析攻击就是指密码分析者通过分析密文和明文的统计规律来破译密码。*

统计分析攻击在历史上为破译密码作出过极大的贡献。许多古典密码都可以通过统计分析而破译。

三、密码学的基本概念

3)*数学分析攻击*　*所谓数学分析攻击是指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，应当选用具有坚实数学基础和足够复杂的加密算法。

三、密码学的基本概念

根据占有的数据资源分类：

A) *仅知密文攻击* (Ciphertext-only attack)

所谓仅知密文攻击是指密码分析者仅根据截获的密文来破译密码。因为密码分析者所能利用的数据资源仅为密文，因此这是对密码分析者最不利的情况。

密码学的基本假设：攻击者总能获得密文。

攻击者总能知道密码算法。

攻击者不知道密钥。

三、密码学的基本概念

根据占有的数据资源分类：

B) *已知明文攻击（Known-plaintext attack）*

所谓已知明文攻击是指密码分析者根据已经知道的某些明文-密文对来破译密码。

攻击者总是能获得密文，并猜出部分明文。

计算机程序文件加密特别容易受到这种攻击。

三、密码学的基本概念

根据占有的数据资源分类：

C) *选择明文攻击* (Chosen-plaintext attack)

所谓选择明文攻击是指密码分析者能够选择明文并获得相应的密文。

计算机文件加密和数据库加密特别容易受到这种攻击。

这是对攻击者最有利的情况！

三、密码学的基本概念

6、密码学的理论基础

(1) 商农信息论

①从信息在信道传输中可能受到攻击，引入密码理论；

②提出以扩散和混淆两种基本方法设计密码；

③阐明了密码系统，完善保密，理论保密和实际保密等概念。

(2) 计算复杂性理论

①密码的安全性以计算复杂度来度量；

②现代密码往往建立在一个数学难题之上，而难是计算复杂度的概念；

③计算复杂度只能为密码提供一个必要条件。

三、密码学的基本概念

7、密码设计的基本方法

(1) 公开设计原则

密码的安全应仅依赖于对密钥的保密，不依赖于对算法的保密。

(2) 扩散和混淆

①扩散(diffusion)：将明文和密钥的每一位的影响散布到尽量多的密文位中；理想情况下达到完备性。

②混淆(confusion)：使明文、密钥和密文之间的关系复杂化。

(3) 迭代与乘积

①迭代：设计一个轮函数，然后迭代。

②乘积：将几种密码联合应用。

三、密码学的基本概念

8、密码学的一些结论：

① 公开设计原则：密码的安全只依赖于密钥的保密，不依赖于算法的保密；

② 理论上绝对安全的密码是存在的：一次一密；

③ 理论上，任何实用的密码都是可破的；

④ 我们追求的是计算上的安全。

⑤计算上的安全：使用可利用的计算资源不能破译。

复习题

① 解释信息安全的含义。

② 密码的基本思想是什么？

③密码体制分哪些类型？各有什么优缺点？

④什么是密码分析？密码分析有哪些类型？

⑤为什么说理论上，任何实用的密码都是可破的？

⑥计算机的程序文件和数据库文件加密容易受到什么攻击？为什么？


谢 谢！