现代密码学

主讲人：谷利泽

Email：glzisc@bupt.edu.cn

Tel:010-62283134

课件下载的信箱

信息安全中心
BuptISC

- 用户：crypto_bupt@sina.com
- 口令：bupt3134

第一讲 绪论

主讲人：谷利泽

Email：glzisc@bupt.edu.cn

Tel:010-62283134

主要内容

- 现代密码学与信息安全的关系
- 现代密码学的主要内容
- 本课程将讲授的内容
- 本课程相关事宜

信息安全

- **信息安全**是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露、否认等，系统连续可靠正常地运行，信息服务不中断。
- 信息安全可分为狭义安全与广义安全两个层次，狭义的安全是建立在以密码技术为基础的计算机安全领域，辅以通信技术、计算机技术与网络技术等方面的内容；广义的信息安全是一门综合性学科，安全不在是单纯的技术问题，而是将管理、技术、法律等问题相结合的产物。

信息安全的主要目标

- 机密性
- 完整性
- 认证性
- 不可否认性

举例说明

- 机密性
  --我与你说话时,别人能不能偷听?
- 认证性
  --我不认识你! -- 你是谁?
  --我怎么相信你就是你? -- 要是别人冒充你怎么办?
- 完整性
  --收到的传真不太清楚?
  --传送过程过程中别人篡改过没有?
- 不可否认性
  --我收到货后,不想付款,想抵赖,怎么样?
  --我将钱寄给你后,你不给发货,想抵赖,如何?

机密性

机密性是指保证信息不泄露给非授权的用户或实体，确保存储的信息和传输的信息仅能被授权的各方得到，而非授权用户即使得到信息也*无法知晓信息内容*，不能使用。

通常通过访问控制阻止非授权用户获得机密信息，通过加密变换防止非授权用户获知信息内容。

完整性

完整性是指信息未经授权不能进行改变的特征，维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改(插入、替换、删除、重排序等)。

一般通过消息摘要算法来验证信息是否被篡改。

认证性

认证性是指确保一个信息的来源或源本身被正确地标识，同时确保该标识没有被伪造，分为实体认证和消息认证。

消息认证是指能向接收方保证该信息确实来自于它所宣称的源。

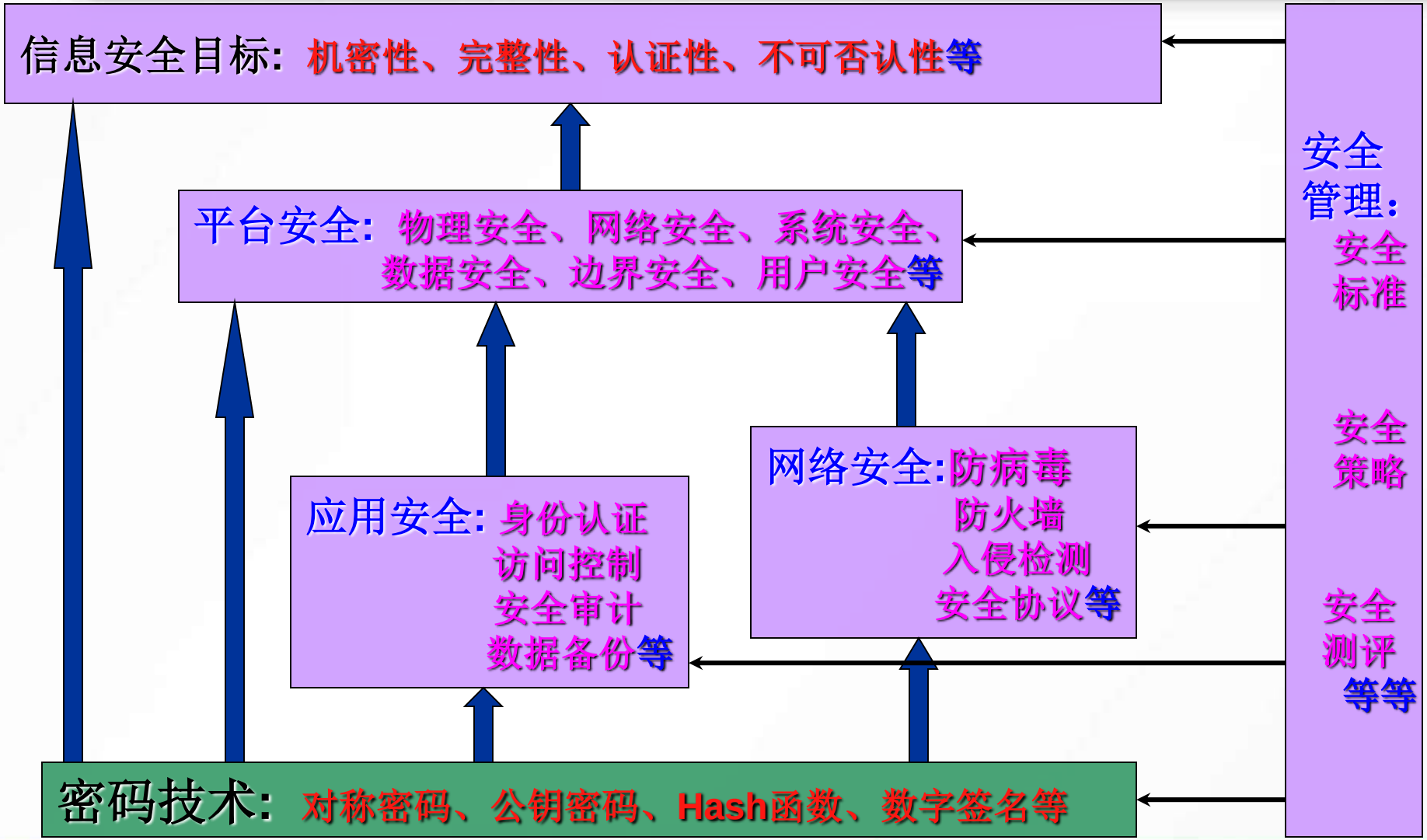
实体认证是指参与信息处理的实体是可信的，即每个实体的确是它所宣称的那个实体，使得任何其它实体不能假冒这个实体。

不可否认性

不可否认性是防止发送方或接收方**抵赖**所传输的信息，要求无论发送方还是接收方都不能**抵赖**所进行的行为。因此，当发送一个信息时，接收方能**证实**该信息的确是由所宣称的发送方发来的；当接收方收到一个信息时，发送方能够**证实**该信息的确送到了指定的接收方。

一般通过**数字签名技术**来实现不可否认服务。

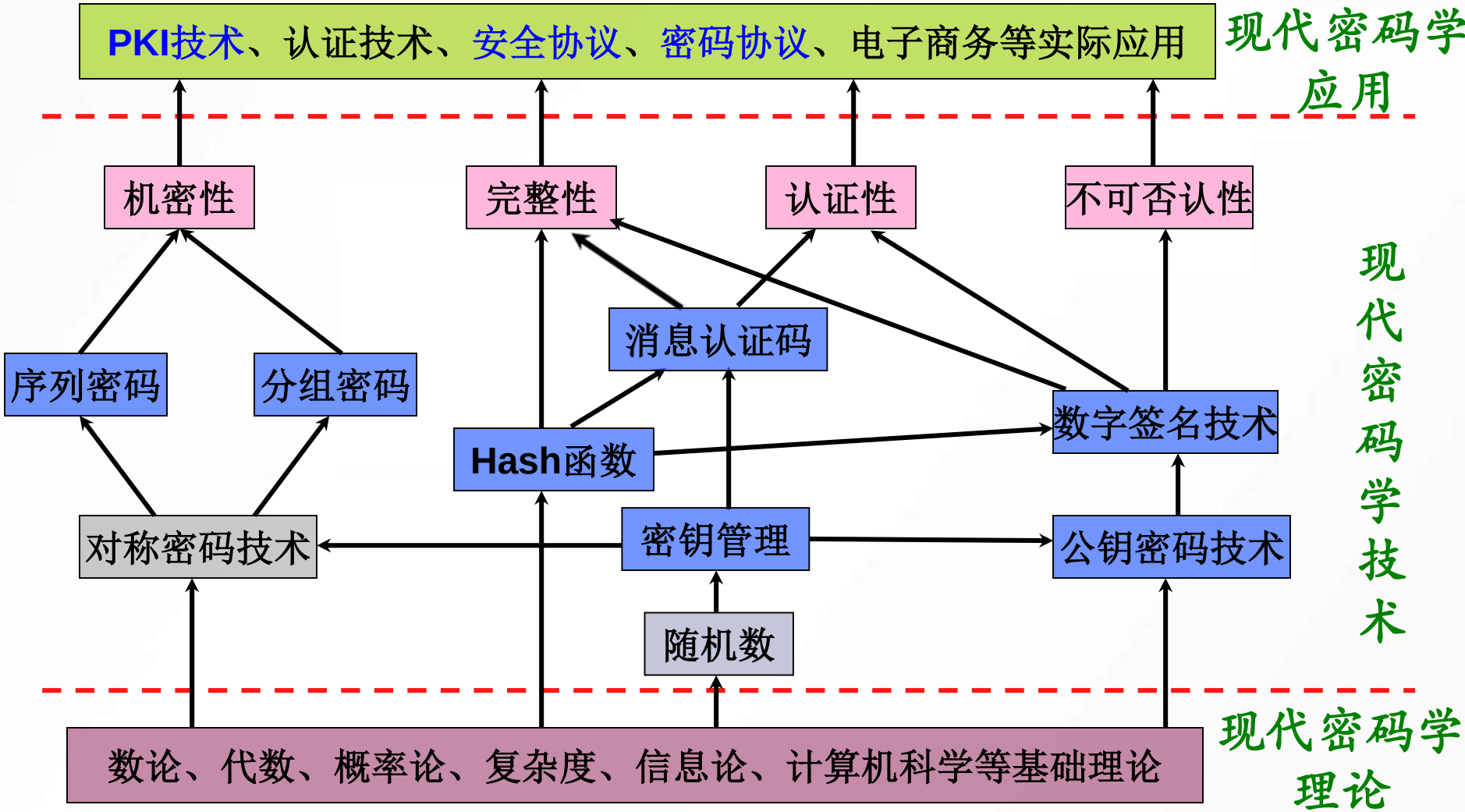
信息安全的主要研究内容



密码学与信息安全

- 密码学是与信息安全各方面（比如机密性、完整性、认证性和不可否认性等）有关的数学技术的研究。
- 密码学是保障信息安全的核心技术，但不是提供信息安全的唯一方式。
- 信息安全是密码学研究与发展的目的。
- 信息安全的理论基础是密码学，信息安全的问题根本解决往往依靠密码学理论。

现代密码学主要研究内容



课程主要内容

- 基础部分（6学时）
- 核心部分（18学时）
- 应用部分（10学时）

基础部分(6学时)

- 绪论(2学时)
- 传统密码技术(2学时)
- 密码学基本知识(2学时)

传统密码技术(2学时)

- 密码学的发展简史
- 置换密码(列置换密码和周期置换密码)
- 代换密码(单表代换密码、多表代换密码和维尔姆密码)
- 典型传统密码的分析(统计分析法和明文-密文对分析法)

密码学基本知识(2学时)

- 密码学的简介
- 简介香农理论
- 密码分析学的基本知识
- 密码系统的安全性

核心部分(18学时)

- 分组密码(4学时)
- 序列密码(2学时)
- 公钥密码(4学时)
- Hash函数及应用(4学时)
- 密钥管理技术(4学时)

分组密码(4学时)

- 分组密码的简介
- DES密码算法
- AES密码算法
- 分组密码的工作方式

序列密码(2学时)

- 序列密码的简介
- 线性反馈移位寄存器
- 非线性序列
- 序列密码的算法举例(A5、RC4等)

公钥密码(4学时)

- 公钥密码体制的简介
- 背包问题
- RSA算法
- ElGamal算法
- ECC算法
- IBE算法

Hash函数及应用(4学时)

- 哈希函数的简介
- 哈希函数算法举例(SHA-1)
- 哈希函数的安全性
- 口令的安全性
- 消息认证
- 数字签名

密钥管理技术(4学时)

- 密钥管理的简介
- 密钥的生命周期
- 公钥证书(亦称数字证书)
- 密钥建立(分配、协商)
- 密钥分割

应用部分(10学时)

- 特殊数字签名(2学时)
- 网络安全协议(2学时)
- 密码协议(4学时)
- 密码学新进展(2学时)

特殊数字签名(2学时)

- 盲签名
- 代理签名
- 多重签名
- 群签名

网络安全协议(2学时)

- 网络安全协议的简介
- 网络安全协议
  - SSL协议
  - SET协议(安全性部分)
  - VPN技术(简介)

密码协议(4学时)

- 零知识认证
- 掷硬币协议
- 比特承诺
- 安全多方计算
- 电子投票
- 电子拍卖
- 电子货币

密码学新进展(2学时)

- 简介量子密码
- 简介混沌密码
- 简介基于格的公钥密码

课程教材

普通高校教育“十一五”国家级规划教材

信息安全专业系列教材

现代密码学教程(第2版)

谷利泽 郑世慧 杨义先 编著

北京邮电大学出版社

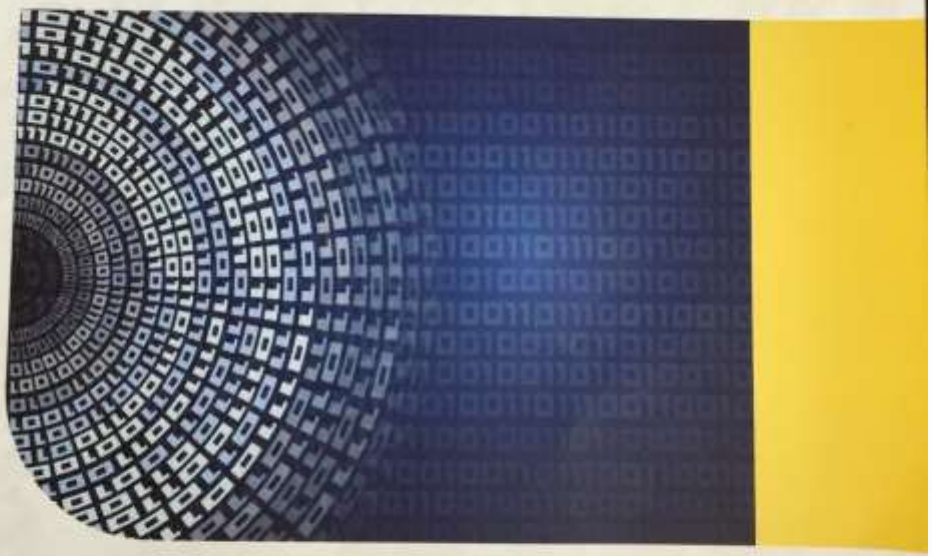
普通高等教育"十一五"国家级规划教材
信息安全专业系列教材

现代密码学教程

MODERN CRYPTOGRAPHY

谷利泽 郑世慧 杨义先 ⊙ 编著

（第2版）



北京邮电大学出版社
www.buptpress.com

课程目标

- 了解现代密码学的基础理论
- 掌握现代密码学的基本技术
- 理解现代密码学的具体应用

把握其核心思想和本质

能够灵活运用所学的知识解决实际中遇到的安全问题

其它事宜

- 现代密码学与其它学科有一定的关联性。
- 定位这门课(基础性的课程)要恰当。
- 考核方式

  闭卷

去年考试题型

一、基础知识部分（40分）

(1)是非判断题（10分)

(2)选择题（15分)

(3)填空题（15分)

二、术语解释（15分）

三、简答题（30分）

四、综合分析题（15分）

本讲小结

- 现代密码学与信息安全的关系
- 现代密码学的主要内容
- 本课程将讲授的内容
- 本课程相关事宜

谢 谢 ！