课件下载的信箱

信息安全中心
BuptISC

- 用户：crypto_bupt@163.com
- 口令：bupt1234

现代密码学

主讲人：谷利泽

Email：glzisc@bupt.edu.cn

第一讲 概述

主讲人：谷利泽

Email：glzisc@bupt.edu.cn

主要内容

信息安全中心
BuptISC

- 密码的理解及主要功能
- 现代密码学与信息安全的关系
- 现代密码学的基本内容
- 本课程将讲授的内容
- 本课程相关事宜

密码的理解

没有完全清楚这种编码机制的所有细节。

只是身份验证的凭据。

提及“密码”大多数人会想到下面情形：登录淘宝或QQ时需要用户名和密码，刷银行卡消费或取款时需要输入密码等等，这种“密码”跟我们这门课要探讨的“密码”是两码事，应该叫做“口令”（password、passcode、pin）。还有，通常把“神秘的编码”称为密码，譬如DNA 称作“遗传密码”等。

简单来说，密码学（cryptography）是一个非常庞大而复杂的信息处理体系，涉及信息的机密性、完整性、认证性、不可否认性等许多方面，属于信息安全范畴。

简单地说，被告知的事实或知识。

密码技术无时无刻地在保护着我们生活中各种信息的安全，而人们很少注意到它的存在，更鲜有人知道我们为什么需要它，以及它究竟是如何工作的。

譬如银行使用的U盾，网络应用中的数字证书、VPN、https等等。

目前为什么更需要密码

信息安全中心 BuptISC

- 不仅国家(军队、外交)，个人或企事业都有自己的秘密。(客观需求)

  不希望被别人(尤其敌手)知道的信息。

- 目前很多信息处理在计算机网络环境下由计算机完成的。(开放的环境)

  存在信息被泄漏、伪造、篡改、否认等风险。

- 为了解决众多实际问题，人们开发出形形色色的密码技术。(满足不同的需求)

  譬如加解密、Hash函数、MAC码，数字签名等等。

密码已经不再仅仅属于专家和研究人员，而是我们每一个生活在现代社会的人都要掌握或了解的一门基本技术。

密码主要功能(举例说明)

信息安全中心
BuptISC

- 机密性
  --我与你说话时,别人能不能偷听?
- 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?
- 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?
- 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*，不能利用。

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)，如果发生，能够及时发现。

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，同时确保该标识的真实性，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。也即是说，当发送方发送一个信息时，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。

主要内容

- 密码的理解及主要功能
- 现代密码学与信息安全的关系
- 现代密码学的基本内容
- 本课程将讲授的内容
- 本课程相关事宜

信息安全

信息的表现形式和载体，可以是符号、文字、数字、语音、图像、视频等。

- 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、泄露、更改、假冒、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。

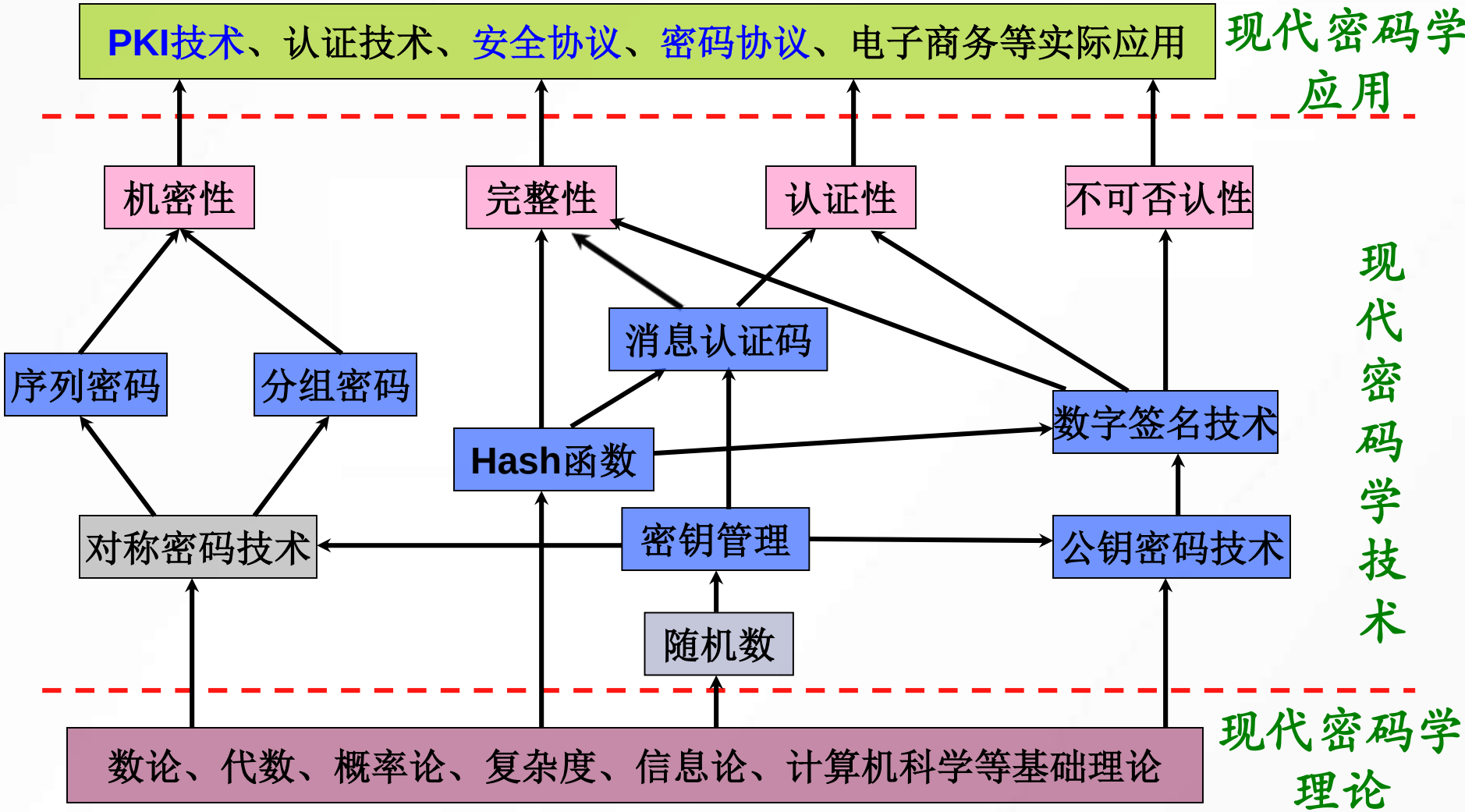
密码与信息安全

- 密码学是与信息安全多方面（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通常依靠密码学理论。

主要内容

- 密码的理解及主要功能
- 现代密码学与信息安全的关系
- 现代密码学的基本内容
- 本课程将讲授的内容
- 本课程相关事宜

现代密码学基本内容


PKI技术、认证技术、安全协议、密码协议、电子商务等实际应用
现代密码学应用
机密性
完整性
认证性
不可否认性
消息认证码
序列密码
分组密码
数字签名技术
Hash函数
对称密码技术
密钥管理
公钥密码技术
随机数
现代密码学技术
数论、代数、概率论、复杂度、信息论、计算机科学等基础理论
现代密码学理论

主要内容

- 密码的理解及主要功能
- 现代密码学与信息安全的关系
- 现代密码学的基本内容
- 本课程将讲授的内容
- 本课程相关事宜

课程主要内容

- 基础部分（6学时）
- 核心部分（18学时）
- 应用部分（6学时）

基础部分(6学时)

- 概述(2学时)
- 密码入门：传统密码技术(2学时)
- 密码学基本知识(2学时)

密码入门:传统密码技术(2学时)

信息安全中心
BuptISC

- 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)
- 典型密码举例(Enigma)
- 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)

- 密码学的发展简史
- 密码学的简介
- 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)

- 对称密码：分组密码(4学时)
- 对称密码：序列密码(2学时)
- 公钥密码(4学时)
- Hash函数及应用(数字签名)(4学时)
- 密钥管理技术(4学时)

对称密码：分组密码(4学时)

- 分组密码的简介
- DES密码算法
- AES密码算法
- SM4密码算法
- 分组密码的工作方式

对称密码：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、ZUC、RC4)

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(SM2)
- IBE算法

Hash函数及应用（数字签名）(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

应用

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)

应用部分(6学时)

信息安全中心
BuptISC

- 网络安全协议(2学时)
- 密码协议(2学时)
- 密码学新进展(2学时)

网络安全协议(2学时)

信息安全中心
BuptISC

- SSL协议
- PGP协议

密码协议(2学时)

- 零知识认证
- 掷硬币协议
- 比特承诺
- 安全多方计算
- 特殊数字签名(盲签名、双重签名)

密码学新进展(2学时)

- 简介量子密码
- 简介后量子密码
- 简介密码法

主要内容

- 密码的理解及主要功能
- 现代密码学与信息安全的关系
- 现代密码学的基本内容
- 本课程将讲授的内容
- 本课程相关事宜

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

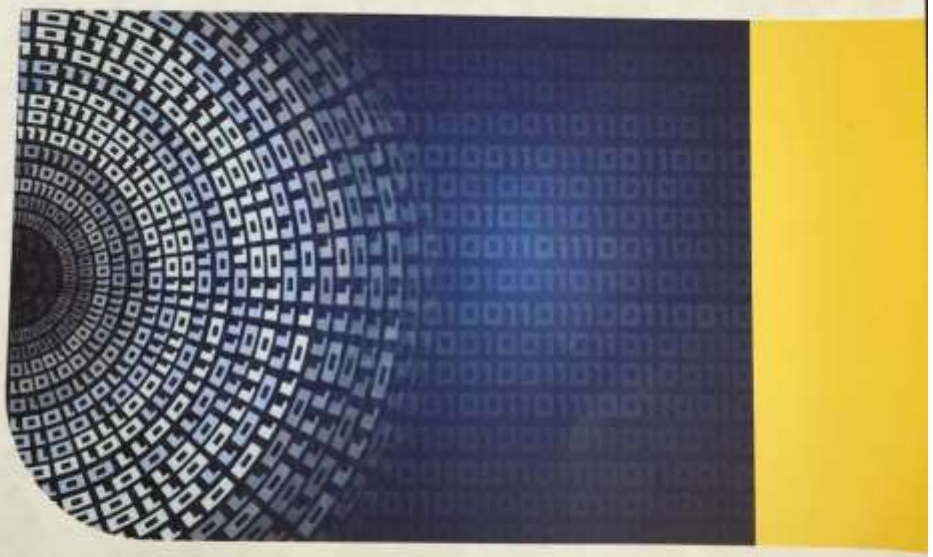
普通高等教育"十一五"国家级规划教材
信息安全专业系列教材

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

进一步学习密码学知识打下坚实的基础

- 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

相关说明

- 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(100%)

本节重点

- 密码的含义及其主要功能
- 现代密码学与信息安全的关系
- 现代密码学的主要内容

答 疑