现代密码学

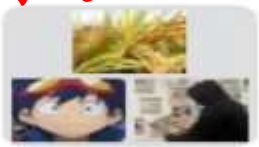
主讲人：谷利泽

Email：glzisc@bupt.edu.cn

扫描下面二维码入群

信息安全中心
BuptISC

进群修改名称：”学号_姓名”



群聊： 现代密码学2024

该二维码7天内(9月16日前)有效，重新进入将更新

第一讲 概述

问题

- 你所认知的密码是什么？

含义？主要内容？主要功能？与网络安全关系？等等

- 这门课将讲授那些内容？

主要内容

- 密码的理解及主要功能
- 现代密码学与网络安全的关系
- 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

简单地说，被告知的事实或知识

只是身份验证的凭据

提及“密码”大多数人会想到下面情形：登录邮箱或淘宝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）。

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。

目前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，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

不希望被别人(尤其敌手)知道的信息。

- 不仅国家(军队、外交等)，个人或企事业都有自己的秘密。
- 目前信息处理主要是在计算机网络环境下由计算机完成的。

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，人们开发出多种多样的密码技术。

譬如消息认证码、数字签名、身份认证等等。

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。

密码法简介

《中华人民共和国密码法》旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，提升密码管理科学化、规范化、法治化水平，是我国密码领域的综合性、基础性法律。

《中华人民共和国密码法》由中华人民共和国第十三届全国人民代表大会常务委员会第十四次会议于2019年10月26日通过，自2020年1月1日起施行。

密码法

信息安全中心 BuptISC

目录

第一章　总　则

第二章　核心密码、普通密码

第三章　商用密码

第四章　法律责任

第五章　附　则

规定了本法的立法目的、密码工作的基本原则、领导和管理体制，以及密码发展促进和保障措施。

规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施。

规定了商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度。

规定了违反本法相关规定应当承担的相应的法律后果。

规定了国家密码管理部门的规章制定权，解放军和武警部队密码立法事宜以及本法的实施日期。

密码主要功能(举例说明)

- 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知晓，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。

通常利用**加密技术**实现机密性

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。

通常利用哈希函数实现完整性

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。 通常采用**消息认证码**实现消息认证

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。

通常采用**数字证书**实现实体认证

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。

通常采用**数字签名技术**实现不可否认性

主要内容

- 密码的理解及主要功能
- 现代密码学与网络安全的关系
- 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

网络安全

信息的表现形式可以是符号、文字、数字、语音、图像、视频等。数据是载荷信息的物理符号。

网络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。

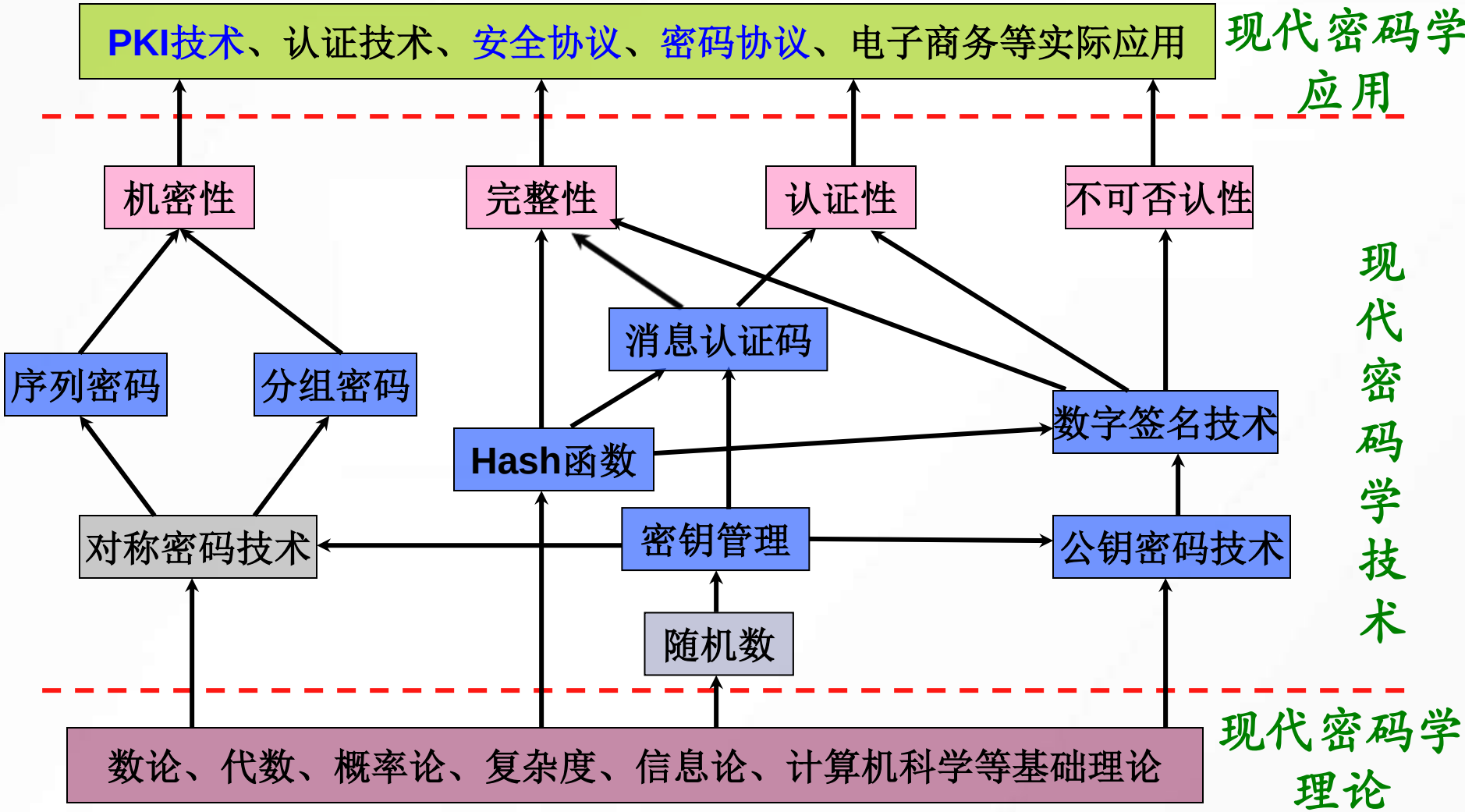
密码学与网络安全

- 密码学是与网络安全多方面（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。
- 密码学是保障网络安全的核心技术，但不是保障网络安全的唯一技术。
- 网络安全是密码学研究与发展的目的。
- 网络安全的理论基础是密码学，网络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
- 现代密码学与网络安全的关系
- 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
- 现代密码学与网络安全的关系
- 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）
  - 对称密码
  - 公钥密码
  - Hash函数及应用
- 应用部分（6学时）

基础部分(6学时)

信息安全中心
BuptISC

- 概述(2学时)
- 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)

- 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)
- 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(6学时)
  - 分组密码(4学时)
  - 序列密码(2学时)
- 公钥密码(6学时)
- Hash函数及应用(消息认证码、数字签名)(6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
- 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(6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)
- SM9算法
- 数字(公钥)证书

Hash函数及应用（消息认证码、数字签名）(6学时)

- 哈希函数的简介
- 哈希函数的安全性
- 哈希函数算法举例(SHA256、SM3)
- 消息认证码
- 数字签名
- 特殊数字签名 (盲签名)

应用

应用部分(6学时)

- 密钥管理(2学时)
- 安全协议及密码协议(4学时)

密钥管理(2学时)

- 密钥管理的简介
- 密钥的生命周期
- 密钥建立(分配、协商)的典型实例
- 数字信封技术

安全协议及密码协议(4学时)

- SSL协议
- 零知识证明
- 比特承诺
- 不经意传输
- 安全多方计算
- 电子投票
- 电子拍卖

主要内容

- 密码的理解及主要功能
- 现代密码学与网络安全的关系
- 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3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

现代密码学教程

MODERN CRYPTOGRAPHY

（第3版）

谷利泽　郑世慧　杨义先　编著

北京邮电大学出版社
www.buptpress.com

课程目标

能够举一反三，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
- 理解现代密码学的实际应用

运用所学的知识解决实际中遇到密码方面的问题

考核方式

通过学校的“教学云平台”上交作业

8次，每次5分

作业(40%)+ 闭卷(60%)

作业内容是考试范围内

判断题、选择题、术语解释、填空题、简答题、综合题等

小结

- 密码的含义及其主要功能
- 现代密码学与网络安全的关系
- 现代密码学的主要内容

答 疑