现代密码学

主讲人：郑世慧

《现代密码学》第一讲

绪 论

课程信息

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

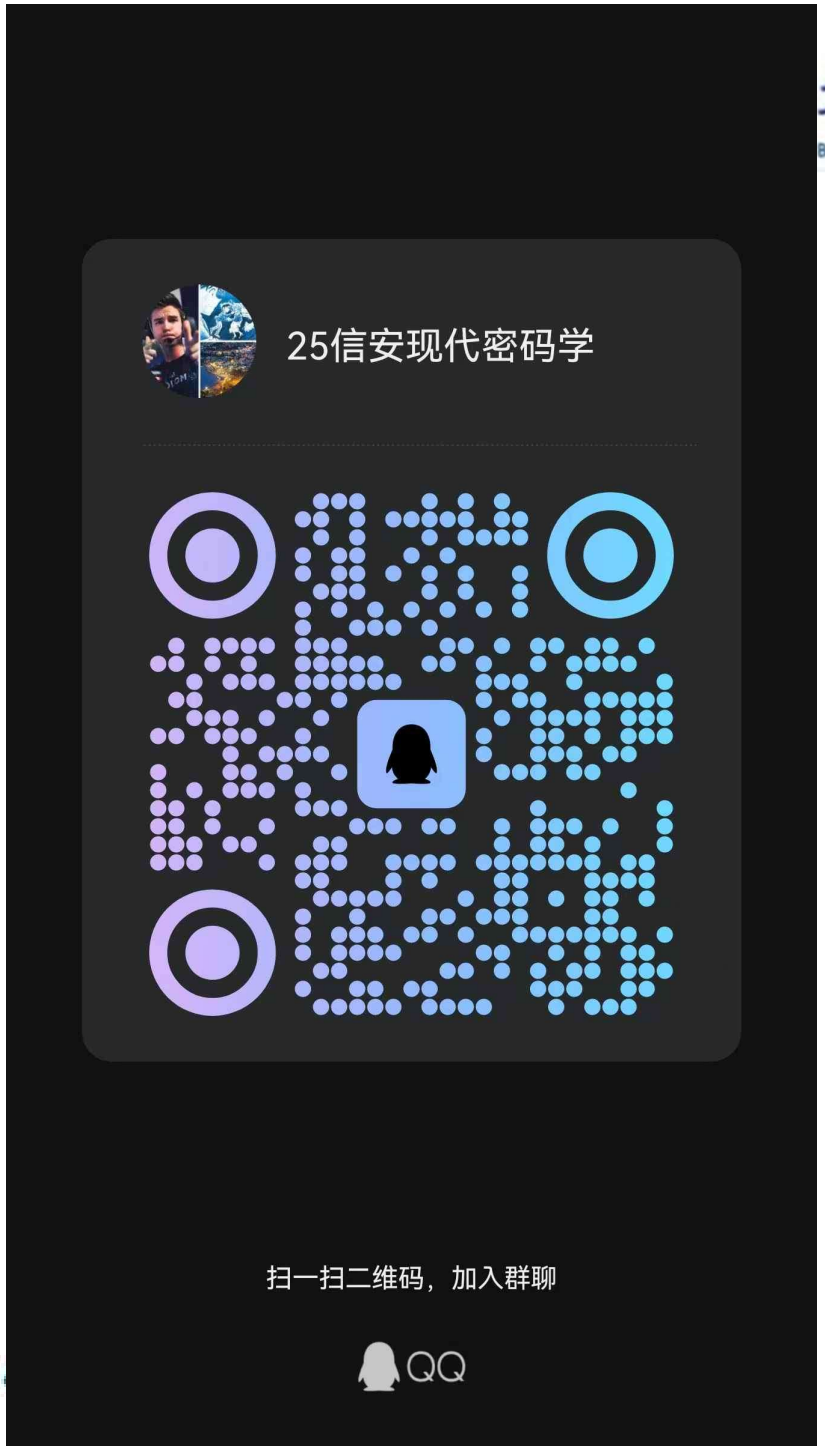
- 课程名称：现代密码学（必修课，考试）共16周
- 任课教师：郑世慧shihuizh@bupt.edu.cn,
- 时间/地点：

  周二下午　教学实验综合楼 N208 15:40- 18:10

（15:40-16:25，16:35～17:20，17:25～18:10）

- 班级：2023211801-2023211802班，2024281801班

课程信息



课程信息

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 课件及每讲作业在教学云平台发布
- 作业：每讲（章）交一次作业

  每讲结束后，下一周周日24：00前截止
- 交作业方式：

https://ucloud.bupt.edu.cn/

考核方式：

平时考勤+作业		15%
随堂考试		25%
期末考试	闭卷考试	50%

参考书目

- 现代密码学教程，谷利泽等，北邮出版社，2015.
- Schneier, Bruce (1996). *Applied Cryptography*, 2ed, Wiley, (ISBN 0-471-11709-9).
- A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone (1996). *Handbook of Applied Cryptography* ISBN 0-8493-8523-7 (online version).
- Mao, Wenbo (2004).*Modern Cryptography Theory and Practice* ISBN 0-13-066943-1.
- Smart, Nigel (2004). *Cryptography: An introduction* ISBN 0-07-709987-7 (online version)
- Stinson, Douglas (2005). *Cryptography: Theory and Practice* ISBN 1-58488-508-4.
- Katz, Jonathan and Yehuda Lindell (2007). *Introduction to Modern Cryptography*, CRC Press.
- Paar, Christof and Jan Pelzl (2009). *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, ISBN 978-3-642-04100-6.

本讲主要内容

- 密码学的目的
- 密码学的历史
- 现代密码学的分类
- 本课程讲授主要内容

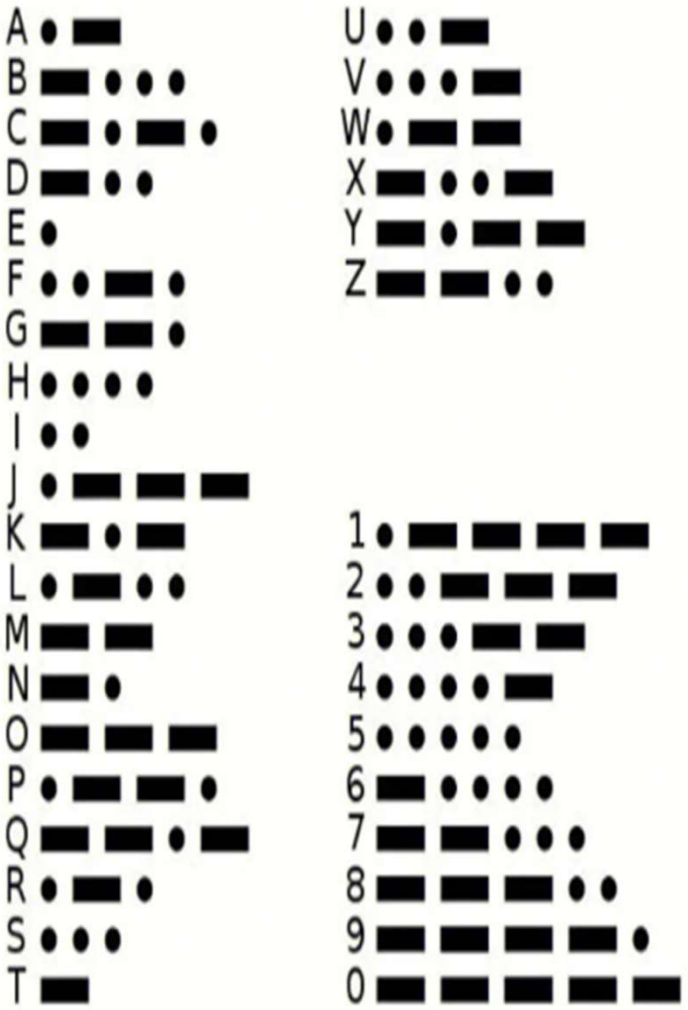
本讲主要内容

- 密码学的目的
- 密码学的历史
- 现代密码学的分类
- 本课程讲授主要内容

密码学的目的

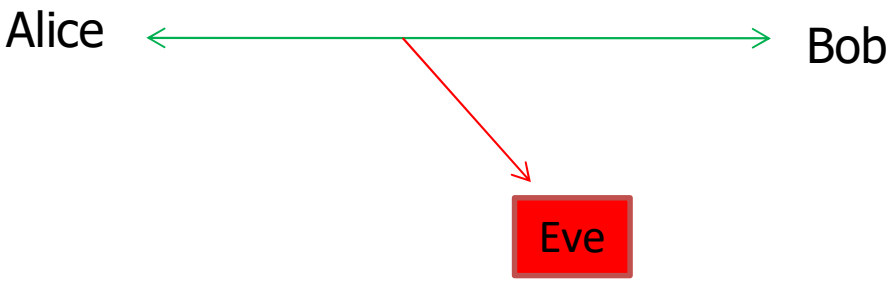
- **2024 年德国军方音频泄露事件**
- **事件概况**：2024 年 3 月 1 日，俄罗斯电视台总编辑西蒙尼扬公布一段时长约 38 分钟的录音，录音日期为 2 月 19 日，涉及德国空军司令格哈茨将军等四名德国空军军官讨论向乌克兰提供“金牛座”巡航导弹的具体细节、如何对克里米亚大桥实施打击等内容。该会议是在美国思科公司的一个商业非加密的在线会议平台上进行的。
- **2025 年西门子 PLC 控制系统被入侵事件**
  事件概况：一条造价上百万的注塑生产线，采用西门子 S7 -1500 PLC 做控制系统。黑客通过工厂内网入侵了 PLC 系统，篡改了多个关键工艺参数，导致车间网络出现异常，设备频繁报警，产品质量出现波动，整条生产线停工。
- **数字签名大盗事件**
  事件概况：数字签名大盗病毒是典型利用数字签名进行恶意攻击的案例。该病毒会修改伪造系统文件 system32.exe，创建名为“系统安全模块（停止可能会引起系统崩溃）”的开机启动项，并指向带有迅雷数字签名的伪造文件。由于带有正规软件签名，能绕过杀毒软件查杀，进而启动真正的病毒文件，导致桌面图标异常、系统主页被修改等问题

密码学的目的

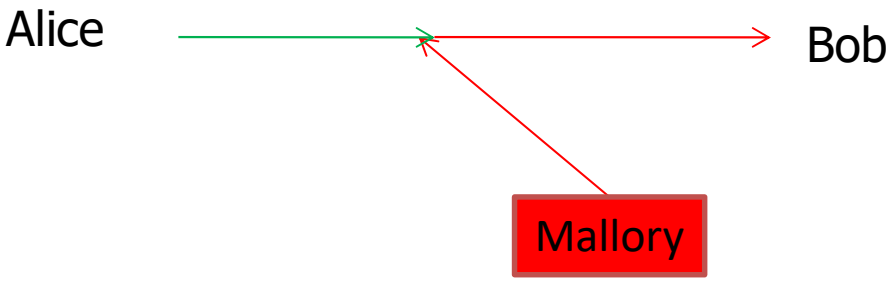


密码学的目的

窃听



插入、篡改



机密性– Confidentiality

完整性–Integrity

可用性– Availability

密码学的目的

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

假冒

对数字信息的签名

认证性–Authentication

(实体认证性、消息源认证性)

不可抵赖性–Non-reputation

BUPT ISC 信息安全中心

密码学的目的

密码学是保障信息安全的核心，信息安全是密码学研究与发展的目的

安全属性（目标）：

- 保密性：信息不泄露给非授权实体
- 完整性：未经授权不能篡改信息
- 实体认证性：实体本身被正确标识
- 不可否认性：用户不能在事后否认信息的生成行为；
- 可用性：保障资源随时可提供服务

本讲主要内容

- 密码学的目的
- 密码学的历史
- 现代密码学的分类
- 本课程讲授主要内容

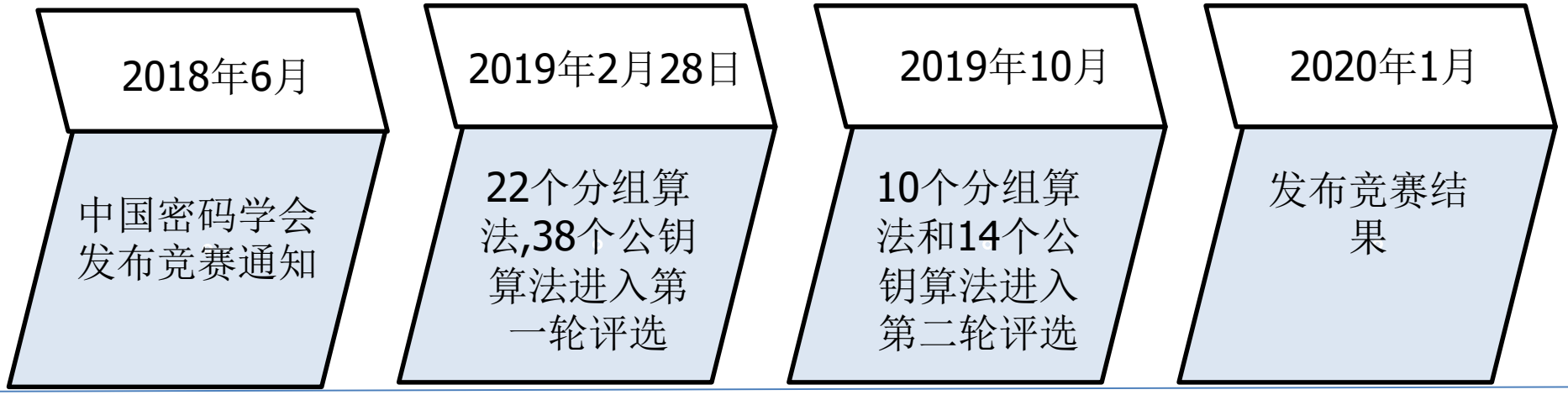
密码学的历史

- 滚筒密码（人类有记载的第一个密码）
- 凯撒密码（古罗马古埃及时代）
- 机械密码(Enigma密码机)
- 香农 1949 “*Communication Theory of Secrecy System* “
- 1976 美国国家标准局(NBS)　DES
- 1976 Diffie-Hellman “*New Direction in Cryptography* ”
- 1978 Rivest、Shamire、Adleman提出第一个实用的密码体制RSA

密码学的历史

- 1997年： 美国标准技术协会(NIST) AES
- 2000年：欧洲密码计划NESSIE(New European Schemes for Signatures, Integnity, and Encryption)
- 2004年：ECRYPT欧洲启动的为期四年的安全项目，其中e-stream评估推荐优秀序列密码方案
- 2008年：hash函数竞赛（secure hash function 3）
- 2014年：CAESAR竞赛（Competition for Authenticated Encryption: Security, Applicability, and Robustness）
- 2016年：后量子密码（Quantum-resistant public-key cryptographic algorithms）
- 新方向：量子密码学、生物密码学

全国密码算法设计竞赛


2018年6月
中国密码学会发布竞赛通知
2019年2月28日
22个分组算法,38个公钥算法进入第一轮评选
2019年10月
10个分组算法和14个公钥算法进入第二轮评选
2020年1月
发布竞赛结果

密码学的历史

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 2004年，电子签章法。
- 《中华人民共和国密码法》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。
- 2019年10月26日下午，十三届全国人大常委会第十四次会议表决通过密码法。自2020年1月1日起施行。

密码学的历史

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

《密码法》核心内容

- 一是密码是什么。
- “是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务”。
- 二是如何分类及应用。
- 密码分为核心密码、普通密码和商用密码。核心密码、普通密码用于保护国家秘密信息；商用密码用于保护不属于国家秘密的信息，公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。
- 三是如何分类管理。坚持党管密码根本原则；对核心密码、普通密码，由密码管理部门依法实行严格统一管理；对商用密码，明确了标准化制度、检测认证制度、市场准入管理制度、关键信息基础设施使用要求、进出口管理制度、电子政务电子认证服务管理制度、行业协会发展要求以及商用密码事中事后监管制度等。
- 四是法律责任。任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统；任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动；明确了对各类密码管理和应用违法行为的处罚措施。

密码学的历史

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

密码学术会议与竞赛

中国密码学会年会
中国密码学会密码测评学术会议
中国密码学会密码数学理论学术会议
中国密码学会密码算法学术会议
中国密码学会量子密码学术会议
中国密码学会区块链密码学术会议
中国密码学会密码芯片学术会议
中国密码学会全国电子认证技术交流大会

全国密码技术竞赛
全国高校密码数学挑战赛
“金融密码杯”全国密码技术大赛

密码学的历史

- 2006年，SMS4算法（WAPI无线网络标准中使用）
- 密码行业标准目录

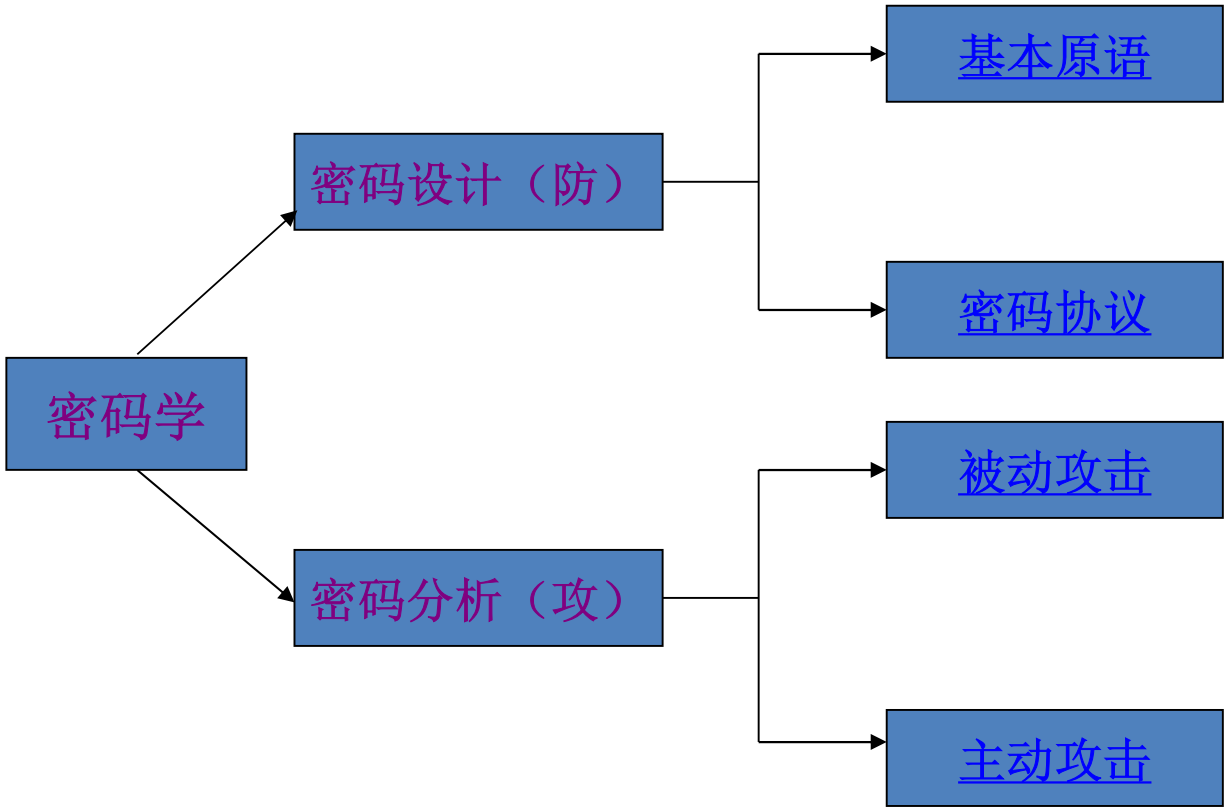
https://www.oscca.gov.cn/sca/xxgk/bzgf.shtml

序号	标准编号	标准名称	主要内容	发布日期	实施日期
1	GM/Z 0001	密码术语	本指导性技术文件给出了商用密码工程领域的基础术语及其定义。本指导性技术文件适用于为密码有关标准、指导性技术文件的编制提供指导，也可用于指导密码技术和产品的论证、设计、生产、使用、检测和评估等。	2013-06-20	2013-06-20
2	GM/T 0001.1	祖冲之序列密码算法 第1部分 算法描述	本部分描述了祖冲之序列密码算法，可用于指导祖冲之算法相关产品的研制、检测和使用。	2012-03-21	2012-03-21

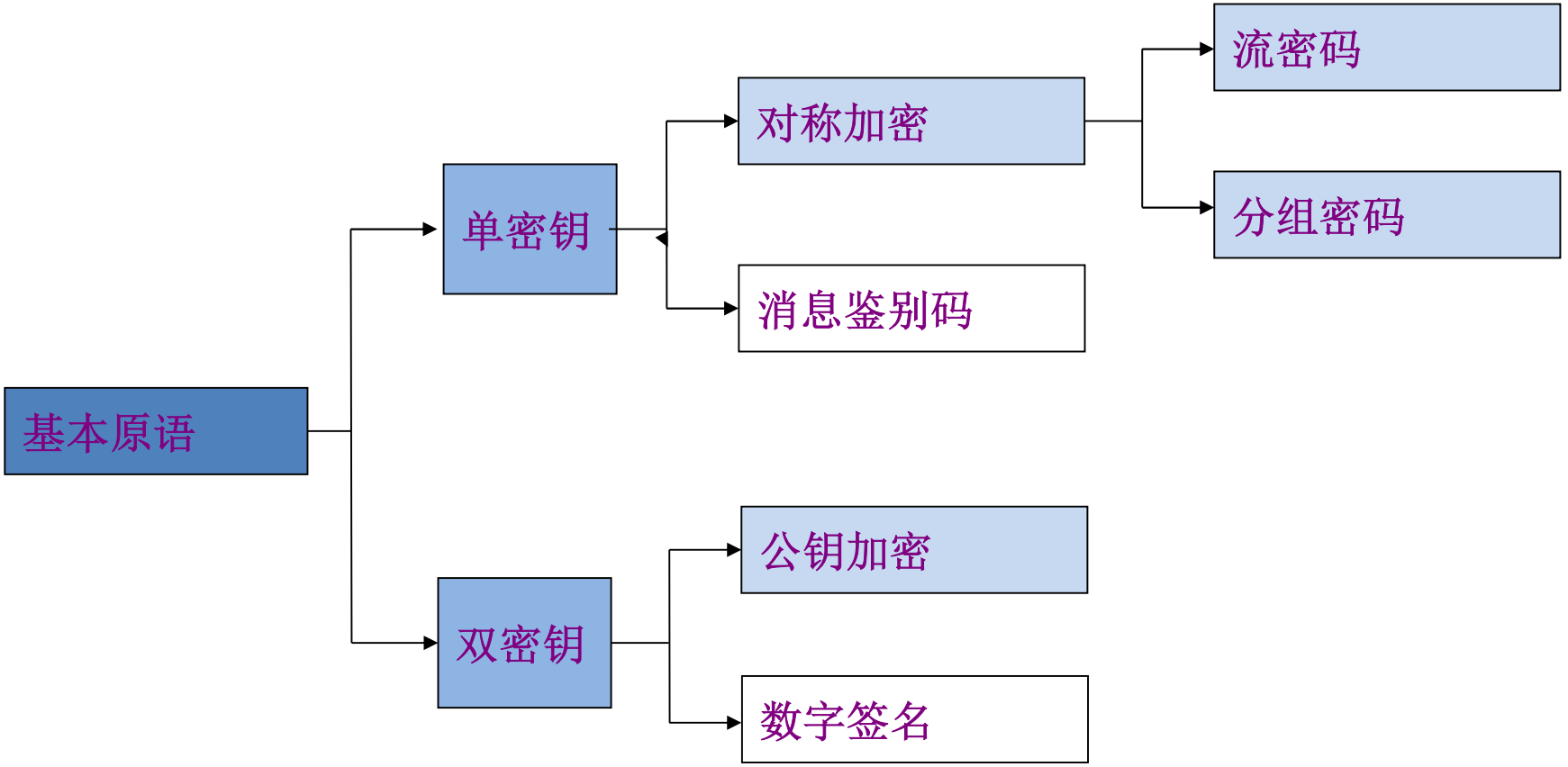
本讲主要内容

- 密码学的目的
- 密码学的历史
- 现代密码学的分类
- 本课程讲授主要内容

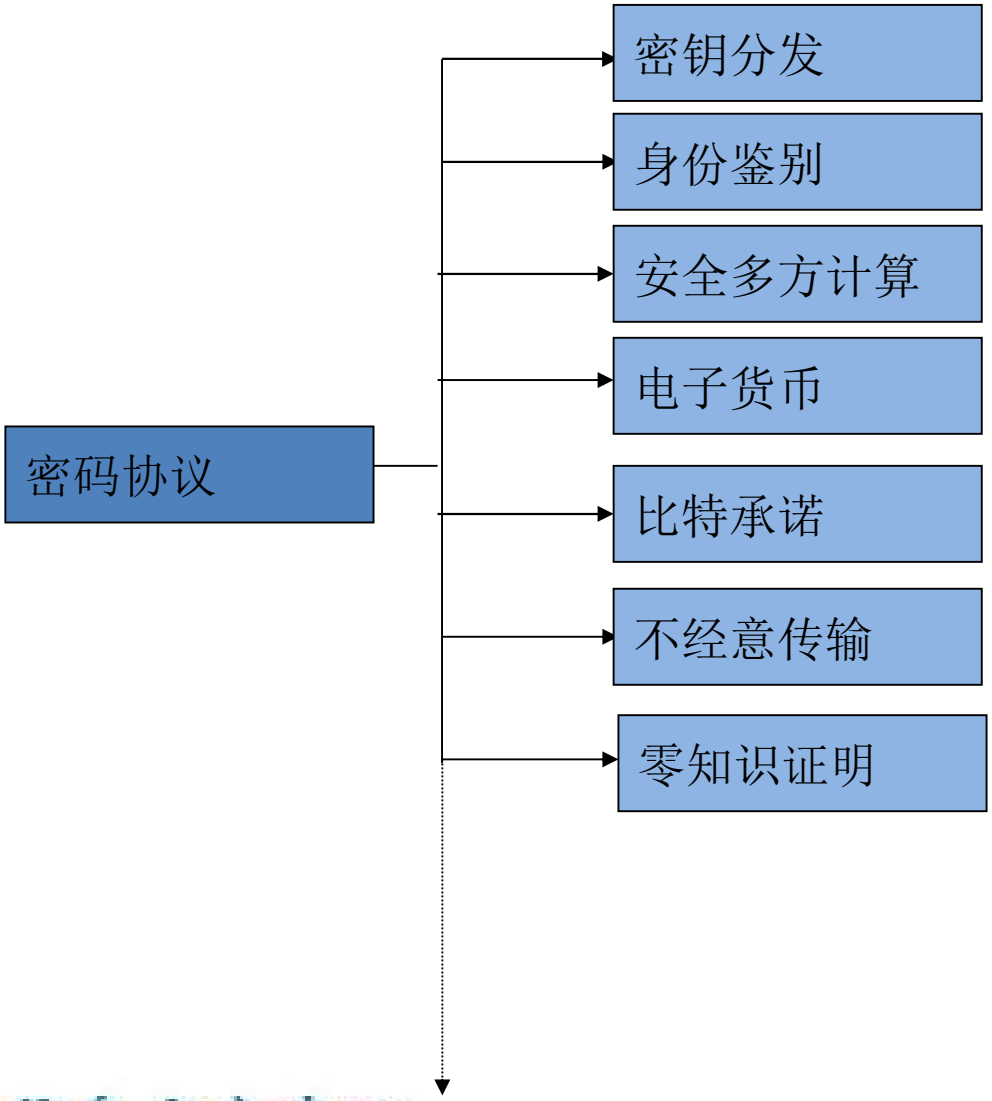
现代密码学的分类



现代密码学的分类



现代密码学的分类



现代密码学的分类

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 被动攻击：

窃听（监听）信道传输的信息，主要危害信息系统的保密性

（轮渡视频）

- 主动攻击：

删除、插入、篡改信道信息，危害完整性、认证性、不可否认性

（钓鱼视频）

现代密码学的分类

- 社会工程学攻击

- 例：力拓门事件

澳大利亚力拓集团驻上海办事处的胡士泰等4名员工涉嫌窃取中国国家机密被拘。

本讲主要内容

- 密码学的目的
- 密码学的历史
- 现代密码学的分类
- 密码分析
- 本课程讲授主要内容

本课程讲授内容

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 第二讲：古典密码学
- 第三讲：密码学基础简介
- 第四讲：分组密码
- 第五讲：伪随机生成器和流密码
- 第六讲：hash函数和消息鉴别码
- 第七讲：公钥加密
- 第八讲：数字签名
- 第九讲：密钥管理
- 第十讲：身份鉴别
- 第十一讲：密码协议
- 第十二讲：量子密码学

主要知识点回顾

- 密码学目的

  安全属性：机密性、完整性、（实体）认证性、不可抵赖性、可用性。

- 密码学分类

  密码编码&密码分析

  对称(分组密码\流密码;消息鉴别码)

  非对称(公钥加密;数字签名)

  被动攻击;主动攻击

THE END !