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

- 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@gmail.com
- 时间/地点：
  周二上午 10:00—11:50　教学实验综合楼S522
  周四上午(单) 8:00—9:50 教学实验综合楼S522
- 学生班级： 2016211322

课程信息

- 作业：每讲交一次作业
- 交作业方式 http://10.109.32.208
- 第一周，默认用户名和口令都为学号；
  - 之后每次作业会在网站发布；
  - 完成的作业以电子版方式上传到网站；
  - 文件名：第*讲_*姓名* _*学号*.
- 考核方式：

平时作业	10%- 15%
期中考试	10%- 15%
课程设计	10%- 20%
期末考试	闭卷考试 60%

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

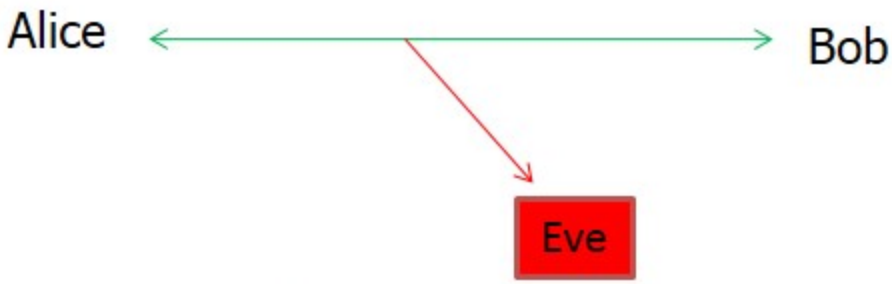
本讲主要内容

- 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

密码学的目的

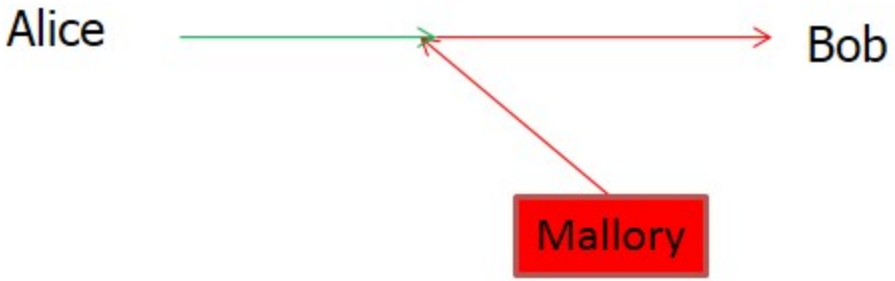
窃听



机密性– Confidentiality

完整性–Integrity

插入、篡改



可用性– Availability

密码学的目的

假冒

对数字信息的签名

认证性–Authentication

不可抵赖性–Non-reputation

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
- 认证性：消息来源或实体本身被正确标识
- 完整性：未经授权不能篡改信息
- 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 美国标准技术协会(NIST)　AES
- 新方向：量子密码学、生物密码学

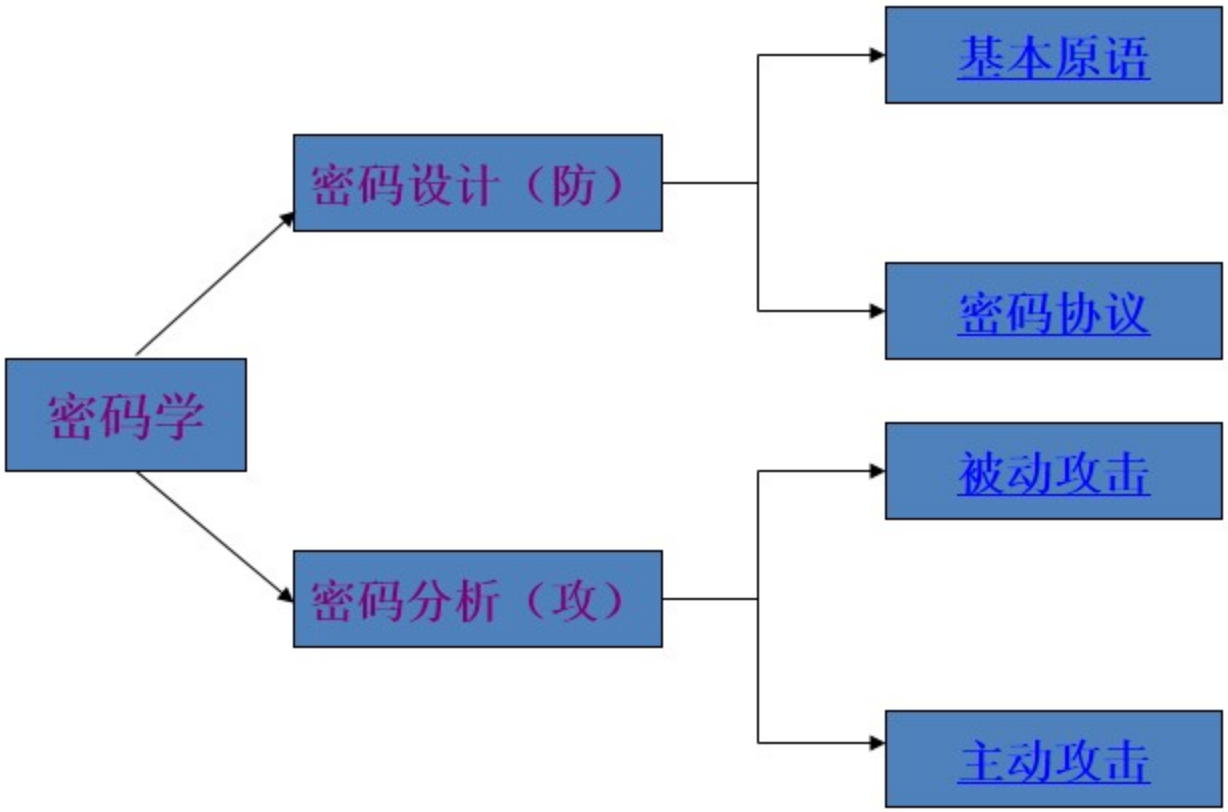
……

- 2004年，电子签章法
- 密码行业标准目录
  http://www.oscca.gov.cn/Column/Column_32.htm

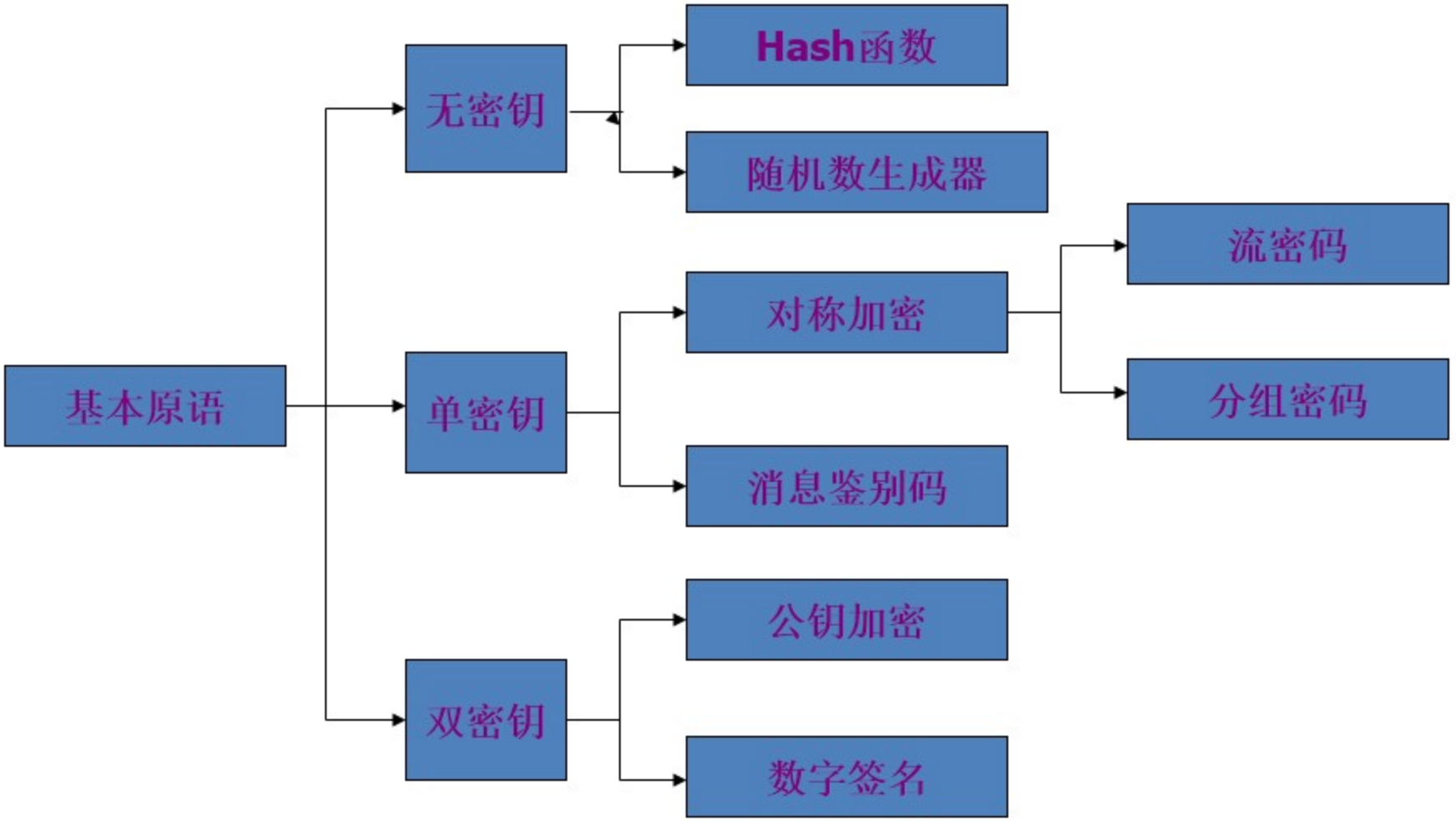
本讲主要内容

- 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

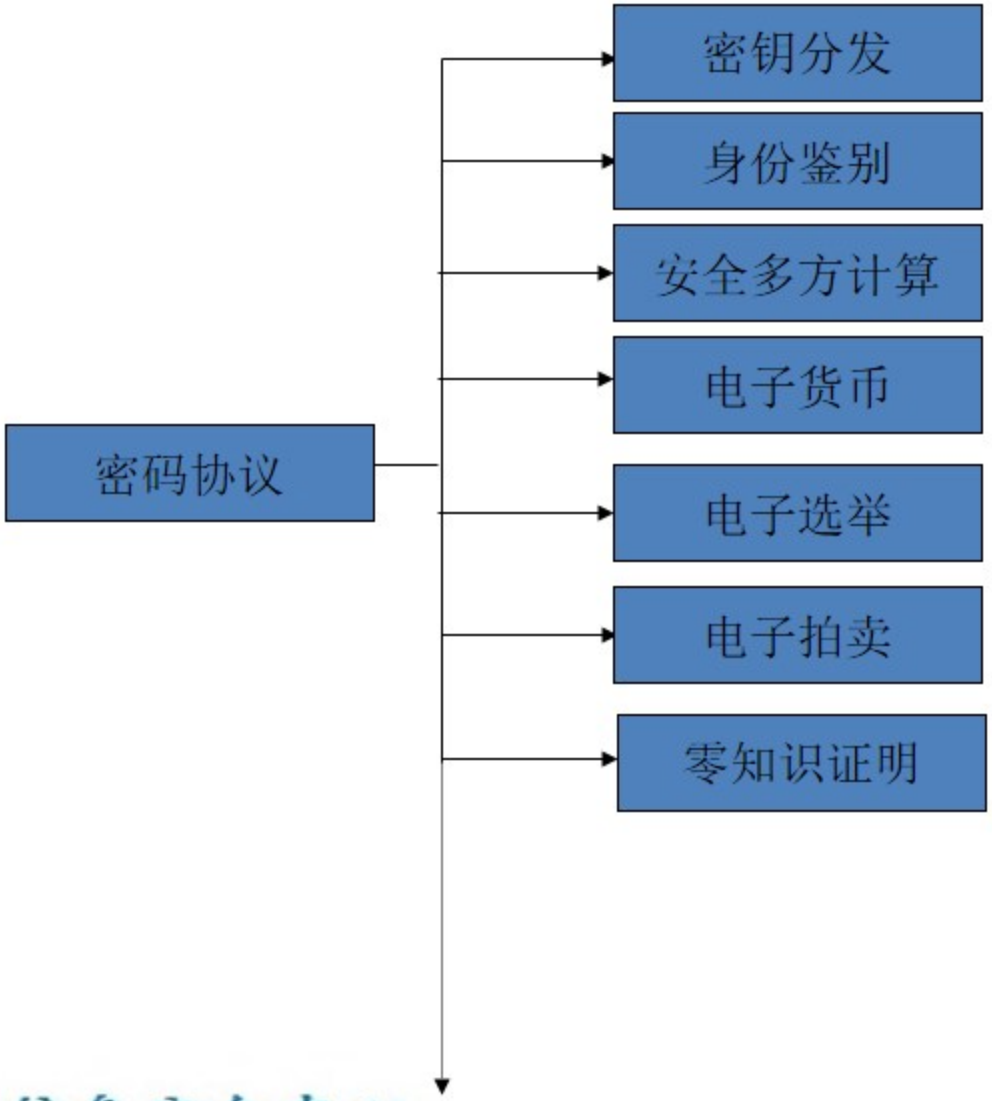
现代密码学的分类



现代密码学的分类



现代密码学的分类



现代密码学的分类

- 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
- 我国商用密码法规

本课程讲授内容

- 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：流密码
- 第六讲：hash函数和消息认证码
- 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

  五个安全属性（机密性、完整性、认证性、不可抵赖性、可用性）

- 密码学分类

THE END!