《现代密码学》第一讲

绪 论

《现代密码学》第一讲

密码学的历史和分类

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
- 《现代密码学》课程讲授主要内容
- 我国商用密码法规

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）
- 两次世界大战的密码战（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

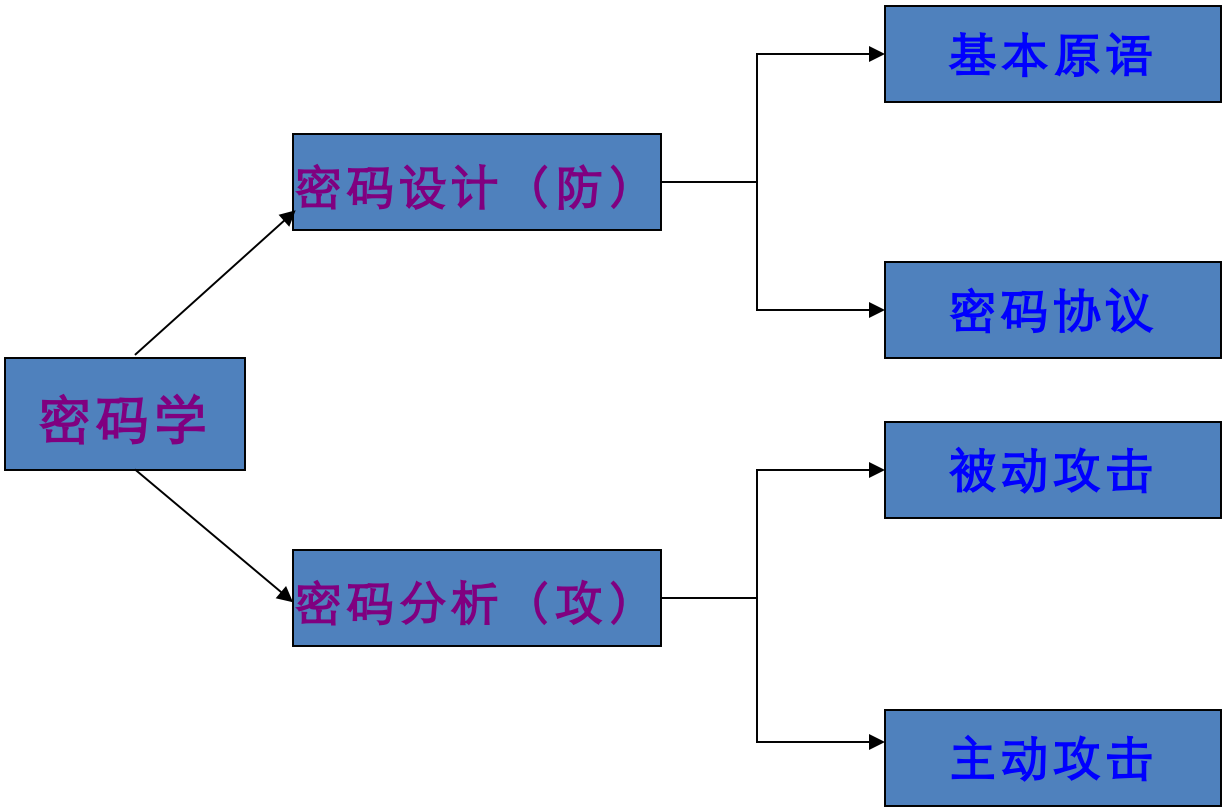
密码学的历史

- 1997 美国标准技术协会（NIST） AES
- 可信计算 采用密码技术自主研制开发的可信计算密码模块（TCM）和密码支撑平台，有效地保障了计算机系统、数据域应用安全
- 混沌密码学
- 量子密码学
- 生物密码学

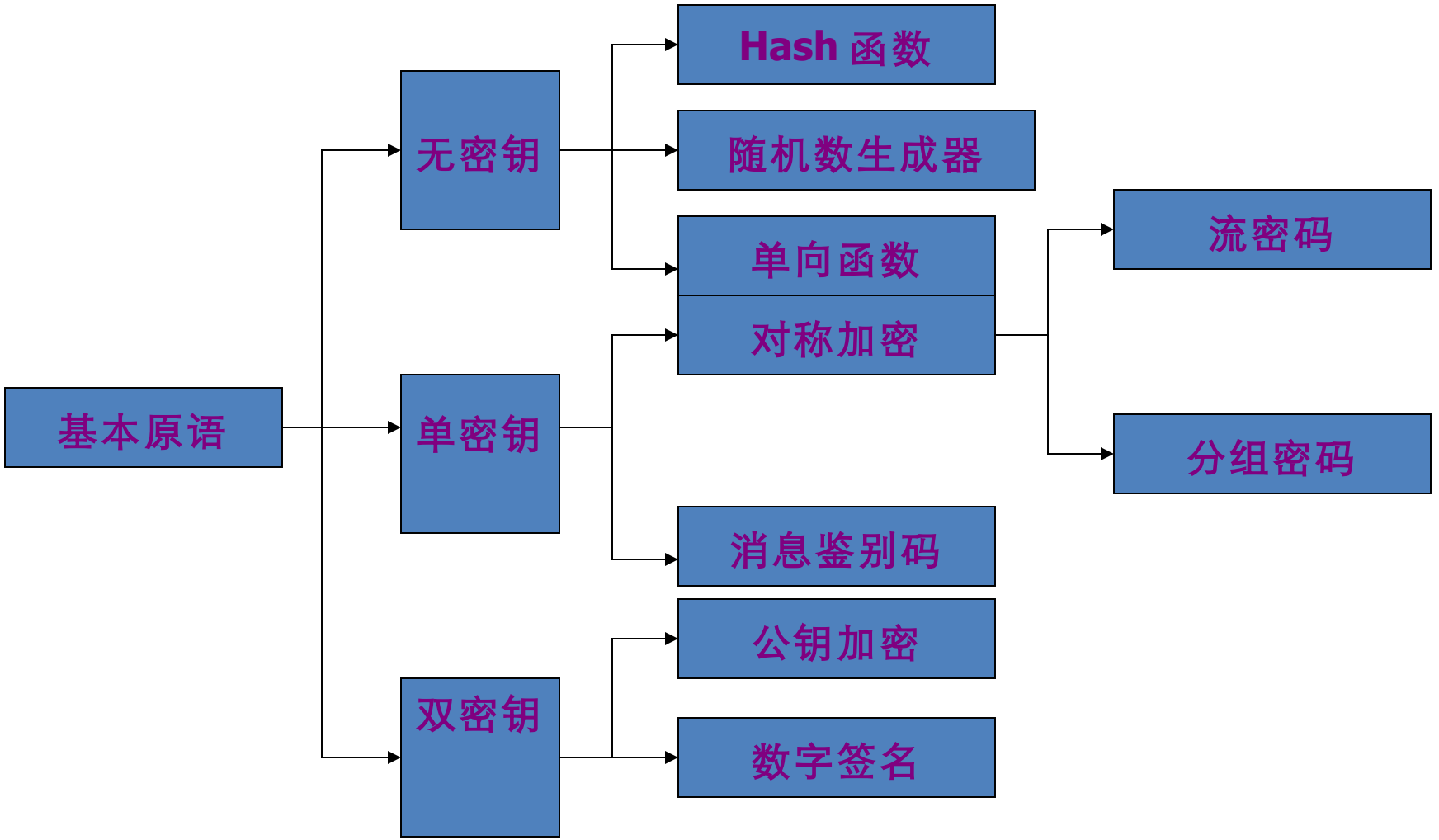
本讲主要内容

- 密码学的目的
- 密码学的历史
- **现代密码学的分类**
- 密码分析
- 《现代密码学》课程讲授主要内容
- 我国商用密码法规

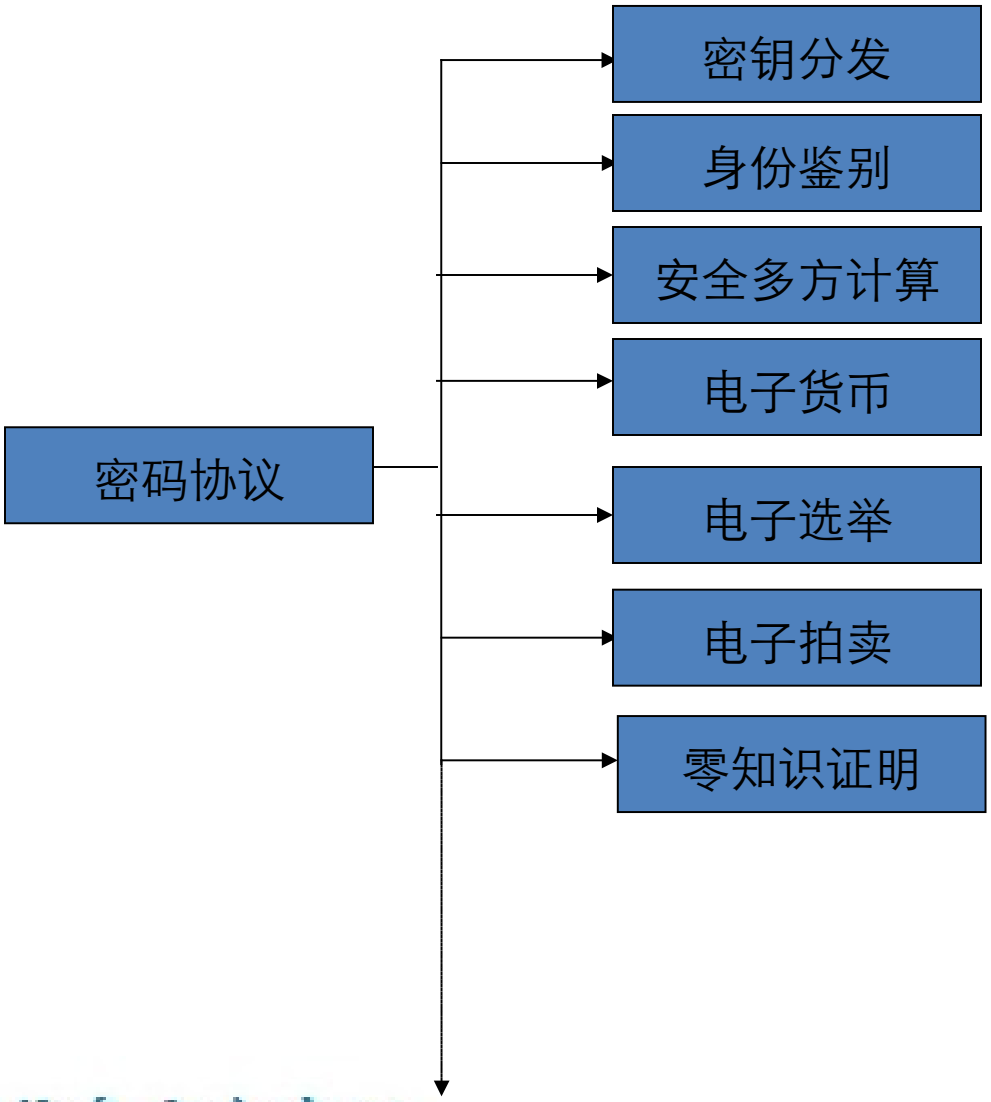
现代密码学的分类



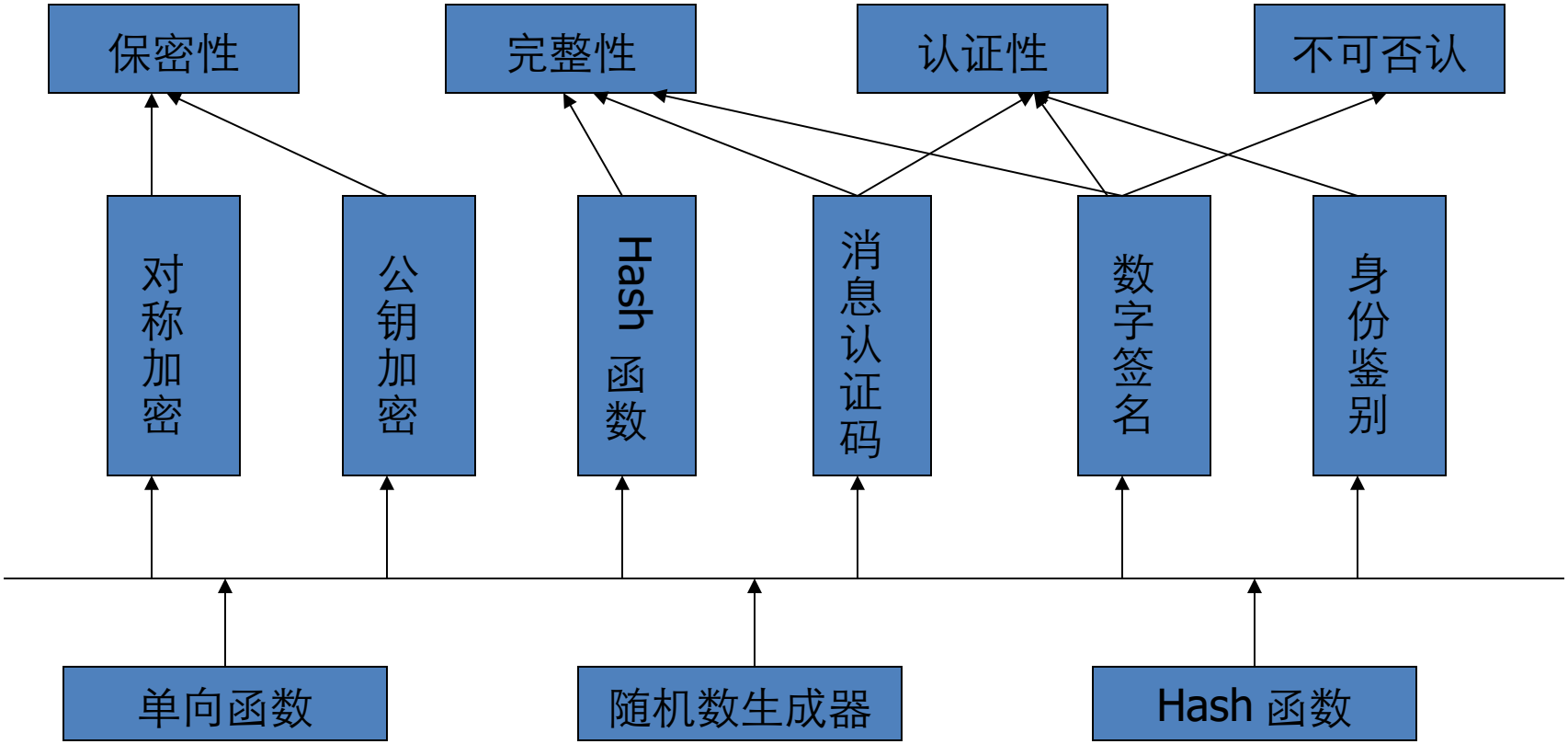
现代密码学的分类


基本原语
无密钥
单密钥
双密钥
Hash 函数
随机数生成器
单向函数
对称加密
消息鉴别码
公钥加密
数字签名
流密码
分组密码

现代密码学的分类



现代密码学的分类


保密性
完整性
认证性
不可否认
对称加密
公钥加密
Hash 函数
消息认证码
数字签名
身份鉴别
单向函数
随机数生成器
Hash 函数

本讲主要内容

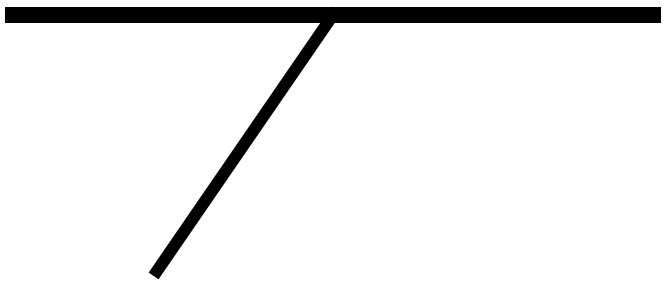
- 密码学的目的
- 密码学的历史
- 现代密码学的分类
- **密码分析**
- 《现代密码学》课程讲授主要内容
- 我国商用密码法规

密码分析

- 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

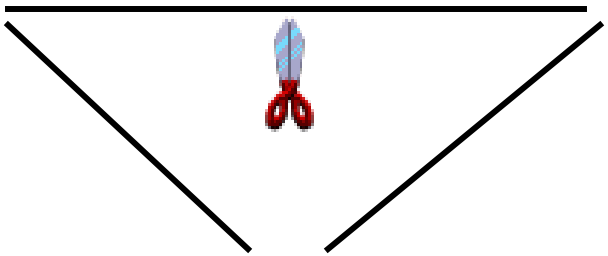
（轮渡视频）



- 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）



密码分析

- 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
- **《现代密码学》课程讲授主要内容**
- 我国商用密码法规

《现代密码学》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：密码协议
- 第十一讲：身份鉴别
- 第十二讲：量子密码学

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
- 《现代密码学》课程讲授主要内容
- **我国商用密码法规**

我国商用密码相关法规

- 密码行业标准目录
- 电子签章法
- 电子认证服务密码管理办法2005
- 电子认证服务密码管理办法2009

- 商用密码管理条例
- 商用密码科研管理规定商用密码产品生产管理规定
- 商用密码产品使用管理规定
- 商用密码产品销售管理规定
- 境外组织和个人在华使用密码产品管理办法

主要知识点回顾

- 密码学分类
- 密码学与信息安全的关系

THE END !