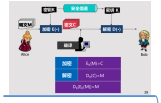
密码学简介

- 加密体制
  - 形式化描述
    - 五元组(P,C,K,E,D)
      - P：明文空间：所有可能的明文组成的有限集
      - C：密文空间：所有可能的密文组成的有限集
      - K：密钥空间：所有可能的密钥组成的有限集
      - E：所有加密算法组成的有限集
      - D：所有解密算法组成的有限集
  - ★ 加密函数
    - 单向函数
      - 是否存在真正的单向函数一直是人类历史上的一道哲学问题
      - 说白了就是去容易,回来不可能
- 秘密通信模型
  - 

  - ★ 考点
    - 密钥KEY
      - 用于"交换"密码算法的输入,是一串随机数
      - 假如算法不用密钥
        - 为毛要密钥
          - 如果攻击者知道了算法，他们只需执行该算法即可以恢复出明文
        - 事实证明，攻击者总能通过各种手段发现你用的是哪个算法
    - 口令PASSWORD
      - 用于身份认证
- 为什么要学密码学
  - 学科基础选修 2.5 分学分
  - 历史上的 NB

获得时间	获奖者	获奖原因
1995	Blum	计算复杂度理论，及其在密码学和程序校验上的应用
2000	Andrew.C.C.Yao	计算理论，包括伪随机数生成，密码学与通信复杂度
2002	Rivest、Shamir、Adleman	RSA加密算法
2012	Goldwasser、Micali	可证明安全性理论
2015	Diffie、Hellman	公钥密码学

  - 密码学就网络安全的先修课
  - 上面的根据北京
    - ★ 密码学是信息安全的基础,是铁壁沦和基数支持
- ★ 密码学能力干什么?
  - 机密性
    - 天知地知你知我知
  - 完整性
    - 检测信息是否被篡改
      - 顾客和款高密谋改善给皇立太子遗诏
  - 认证
    - 证明你妈是你妈
  - 匿名性
    - 证明身份的同时,不泄露自己的身份
      - TOR 浏览器
- 信息安全三要素
  - 机密性
    - 社会工程学
  - 完整性
    - 合法用户的失误
      - 非法用户的篡改
  - 可用性
    - 拿锤子砸了服务器
- 实用加密算法必须满足两个条件
  - 容易性
  - 安全性
- ★ 什么是密码学
  - 基本术语
    - 破译密码
      - 密码分析学
    - 密码编码学
      - 设计密码,就们主要学的就是这个
    - 明文
      - 人读的
    - 加密
      - 把人读的东西变成乱码
      - 做品加密后都唱乱码
    - 密文
    - 解密
      - 把乱码变成人读的东西
    - 密码分析
      - 破译密码
- ★ 密码学的主要功能
  - 保证机密性
    - 防窃听
  - 保证完整性
    - 防破坏
  - 提供非否认
    - 区块链
- ★ 攻击者
  - 被动攻击
    - 窃听,破坏机密性
  - 主动攻击
    - 对完整性,可用性的破坏

- 事实证明，攻击者总能通过各种手段发现你用的是哪个算法
  - 视扉无处不在
  - 鸡儿大夫原则
    - 意义
      - 知道算法的的作方一致变了
      - 设计者有个人的思趣味比如我
        - ★ 同等对待所有密钥，不要根据自己的偏好选择密钥（以防攻击者根据你的偏好缩小密钥范围）
      - 密码学理论研究太辛苦了
        - 频繁更换算法不现实
      - 所以说,密码算法是很难保密的
    - "即使密码系统的任何细节已为人所知只要密钥没有泄漏它也应该是安全的"