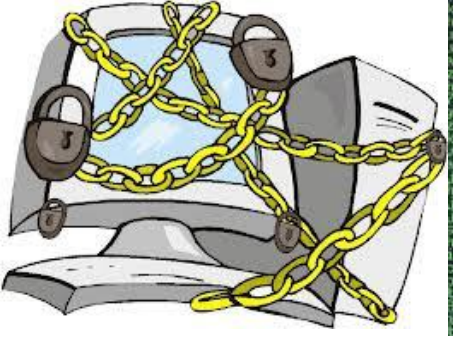



信息系统安全

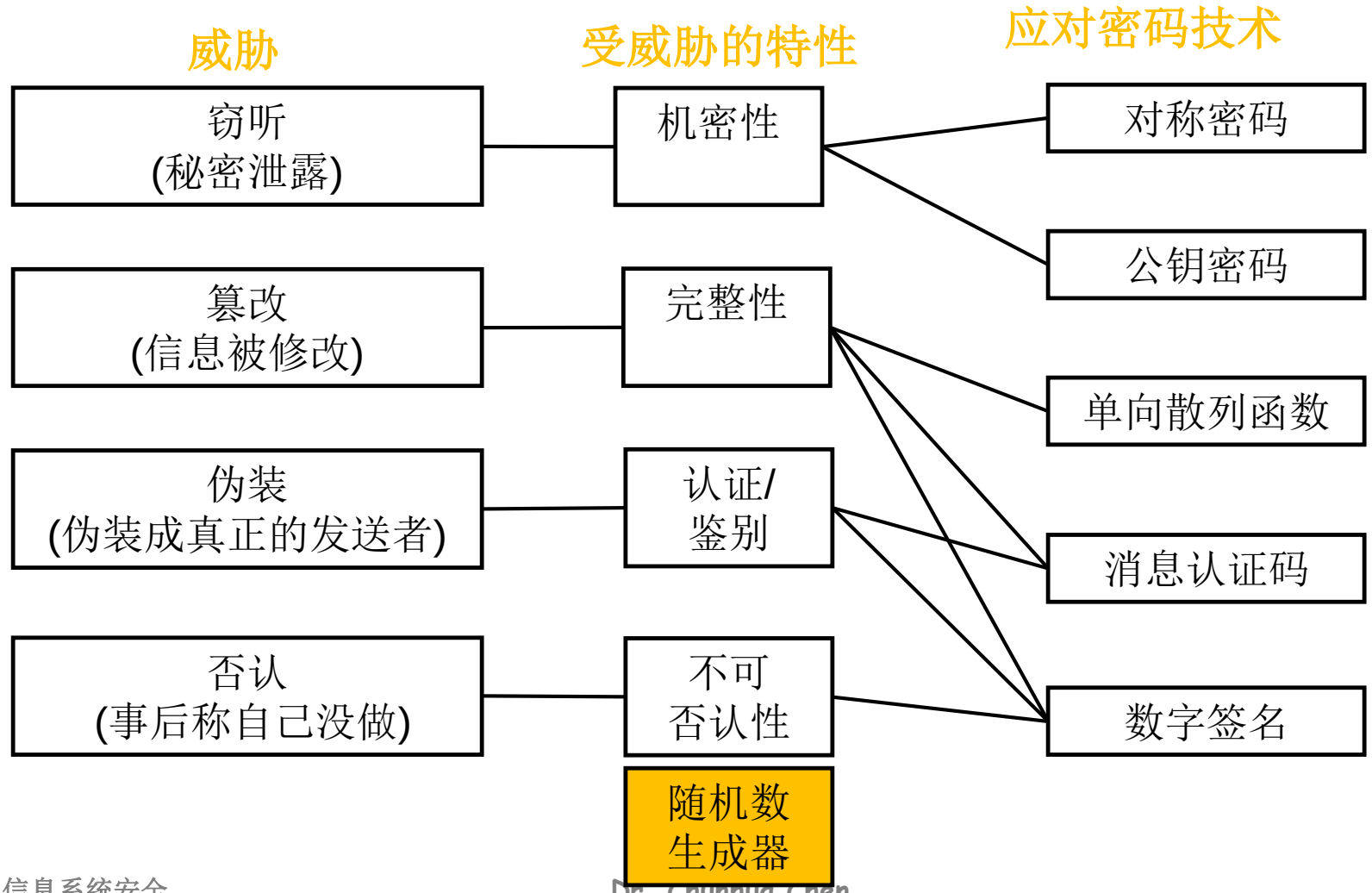
综述

密码技术及其应用

陈春华 博士
chunhuachen@scut.edu.cn

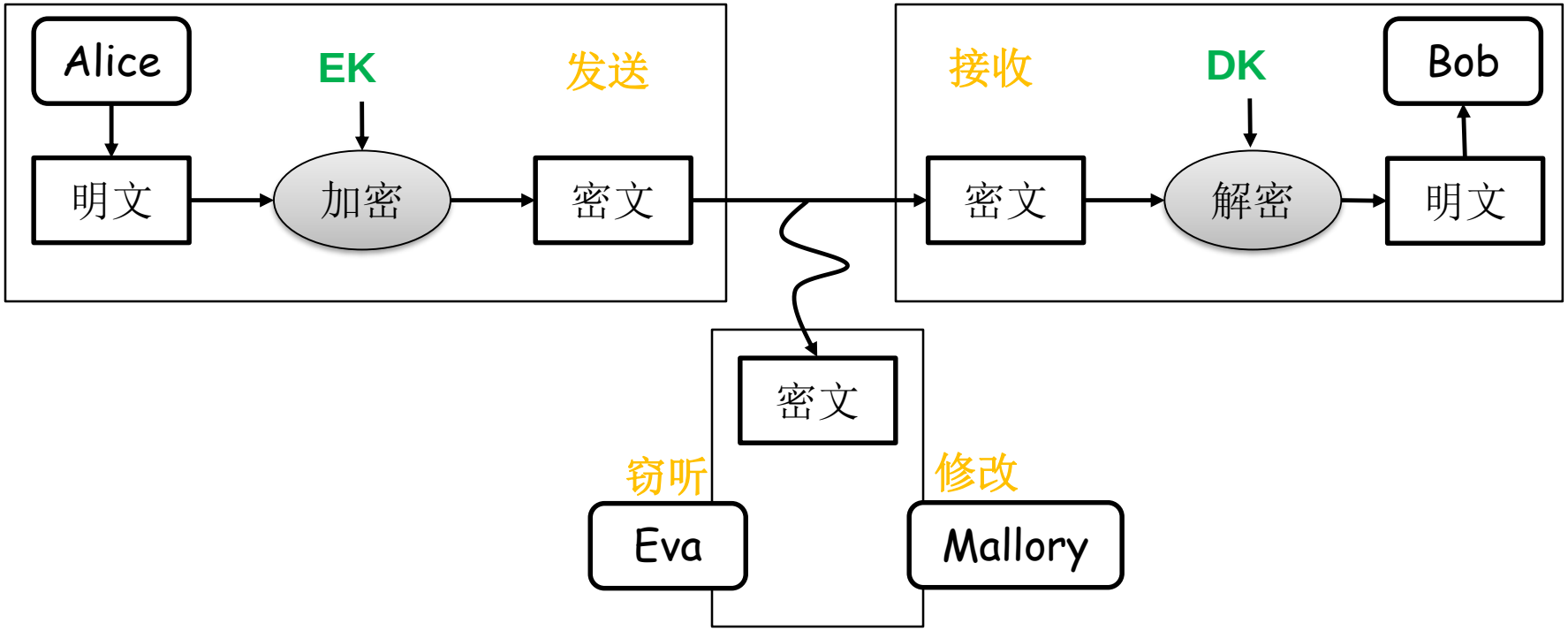
2018 春季
华南理工大学 软件学院

密码学家的工具箱



Dr. Chunhua Chen
chunhuachen@scut.edu.cn

加密与网络安全通信模型



- 密码算法公开，密钥保密持有而且空间足够大；
- 攻击者通常攻击密钥，比如穷举密钥攻击

对称加密

- 加密密钥EK=解密密钥DK
- 加密速度快，适合加密大量数据
- 流密码，其密钥依赖伪随机数生成器产生的密钥流
- 块密码，又称分组密码
  - 块大小与密钥长度
  - 通常对明文块进行迭代，迭代的具体方式称为模式，如CBC等
- DES密码与AES算法
- 对称密码，又称私钥密钥，单钥密码，...

公钥加密

- 加密密钥EK != 解密密钥DK，具有严格的数学关系，又称密钥对
- 加密密钥EK，公开发布，又称公钥
- 解密密钥DK，拥有者保密持有，又称私钥
- 使用接收者公钥加密，使用对应的私钥才能加密
  - 为什么？
- 速度远低于对称密码，适合加密小量数据，如一个对称密钥
- RSA密码系统，黄金标准
- 攻击：除了期望获取对应私钥，还可以进行中间人攻击

密钥配送问题

- 对称密码
  - 在大规模的开放性网络中是个难题
- 非对称密码
  - 公钥公开，没有保密问题
- 解决：
  - 事先共享
  - 通过密钥分配中心(Key Distribution Center, KDC)
  - 通过Diffie-Hellman密钥交换
  - 通过公钥密码
- 公钥密码，一定程度上解决密钥的保密性问题，但是无法解决认证/鉴别问题：如何判断公钥属于谁的？

Diffie-Hellman密钥交换

- 第257页，11.5.2章节

混合密码系统

- 用对称密码提高速度，用公钥密码保护会话密钥~
  - 使用对称密码加密消息
  - 通过伪随机数生成器生成对称密码加密中使用的会话密钥
  - 用公钥密码加密会话密钥
  - 从混合密码系统外部赋予公钥密码加密是使用的密钥对
- 会话密钥：指为本次通信而生成的临时密钥，一般比明文要短很多
- PGP，IPSec和SSL/TLS等都运用了混合密码系统

认证/鉴别-完整性-单向散列函数

- 认证/鉴别
  - 消息源，来自哪里
  - 信息内容，是否被篡改
- 单向散列函数
  - H(M*)=h, 任意长消息到定长消息的映射
- 构造性攻击: H(M1)=H(M2), M1 != M2
  - 抗弱碰撞性，给定M1，进行构造
  - 空强碰撞性，构造M1和M2
- MD5和SHA-1等
- 又称消息摘要，哈希和杂凑函数

- 用途
  - 检测软件是否被篡改
  - 消息认证码
  - 数字签名
  - 伪随机生成器
- 攻击
  - 暴力破解
  - 生日攻击

认证/鉴别-完整性-消息认证码

- MAC(M,K), 与散列函数不同，需要输入共享密钥
  - 使用散列函数构建，称为HMAC
  - 使用分组密码构建，如DES-CBC
- 可认为消息认证码是一种与密钥相关联的单向散列函数
- 面临对称加密系统中相同的密钥配送问题
- 攻击：
  - 重放攻击：序号与时间戳
  - 推测密钥
- 无法解决的问题：
  - 第三方证明
  - 防止否认

数字签名

- 数字签名是根据消息内容生成的一串“只有自己才能计算出来的数值”
  - 生成消息签名与验证数字签名
- 可通过公钥加密系统构建数字签名
  - 私钥加密，即签名
  - 公钥解密，即验证
- 签名方法：
  - 直接对消息签名
  - 对消息的散列值签名
- 应用：安全信息公告/软件下载/公钥证书与SSL/TLS等

- 算法
  - RSA
  - ELGamal
  - DSA
- 攻击
  - 中间人
  - 攻击散列函数
  - 利用数字签名攻击公钥

各种密码技术的对比

	对称密码	公钥密码
发送者	用共享密钥加密	用公钥加密
接受者	用共享密钥解密	用私钥解密
密钥配送问题	存在	不存在，但是公钥需要另外认证
机密性	●	●

	消息认证码	数字签名
发送者	用共享密钥计算MAC	用私钥生成签名
接受者	用共享密钥计算MAC	用公钥验证签名
密钥配送问题	存在	不存在，但是公钥需要另外认证
完整性	●	●
认证	●(仅限通信对象系统)	●(可适用任何第三方)
防止否认	○	●

密钥配送问题：如何实现公钥认证？

- 即使数字签名功能再强大，如果你得到的公钥是伪造的，那么数字签名也完全失效。
- 数字证书与公钥基础设施
  - 引入可信第三方(社会学领域的概念)
  - 数字证书，又称公钥证书，就是将公钥作为一条消息，由一个可信第三方对其签名后所得到的公钥与签名等数据
  - 基础设施：广泛认可并使用
- 公钥基础设施 Public Key Infrastructure, PKI

数字证书

- 公钥证书(Certificate)，包含姓名，组织，邮箱等个人信息，以及属于此人的公钥，并有认证机构(Certification Authority, CA)施加的数字签名。
- 只要看到公钥证书，我们就可以知道认证机构认定该证书中的公钥的确属于证书中声明的实体。
- 认证机构中国际性组织，政府所设立的组织，也有通过提供认证服务来盈利的一般企业等等
  - VeriSign公司
- 证书标准规范 X.509
- 查看浏览器中的证书，windows证书管理器 (certmgr.msc)

公钥基础设施 PKI

- 为了能够更有效地运用公钥而制定的一系列规范和规格的总称。
- PKI的组成要素 (第229页)
  - 用户/实体
  - 认证机构
    - 生成密钥对
    - 注册证书
    - 作废证书与CRL
  - 证书仓库
- 证书的层次结构，证书链
  - 顶级认证机构→下一级

Further Reading: