现代密码学

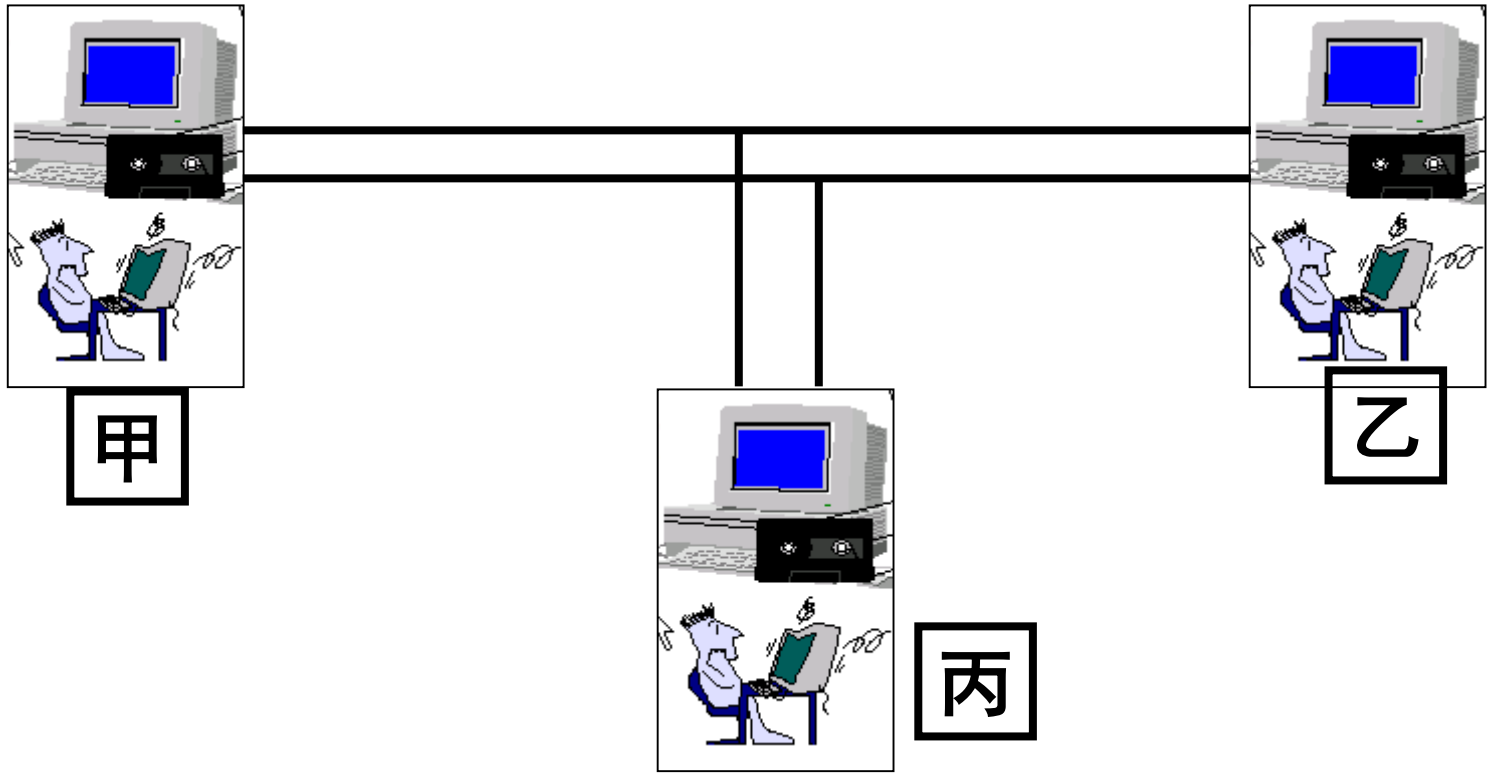
第一讲 密码学的基本概念

信息与软件工程学院

第一讲 密码学的基本概念

- 信息安全的基本属性
- 什么是密码学
- 密码算法的分类
- 密码学的作用和地位

信息安全的基本任务



信息安全的基本属性

- 机密性 （Confidentiality）
  - 保证信息为授权者使用而不泄漏给未经授权者。
  - 别人“看不到”或“看不懂”
- 认证（Authentication）
  - 消息认证，保证消息来源的真实性
  - 身份认证，确保通信实体的真实性
  - 证明“你就是你”
- 完整性 （Integrity）
  - 数据完整性，未被未授权篡改或者损坏
  - 系统完整性，系统未被非授权操纵，按既定的功能运行
  - 信息没有被“动过”

信息安全的基本属性（续）

- 不可否认性（Non-repudiation ）
  - 要求无论发送方还是接收方都不能抵赖所进行的传输
- 可靠性（Reliability）
  - 特定行为和结果的一致性
- 可用性 （Availability）
  - 保证信息和信息系统随时为授权者提供服务，而不要出现非授权者滥用却对授权者拒绝服务的情况。
- 可控性（Controllability）
  - 授权实体可以控制信息系统和信息使用的特性
- 审计（Accountability）
  - 确保实体的活动可被跟踪

第一讲 密码学的基本概念

- 信息安全的基本属性
- 什么是密码学
- 密码算法的分类
- 密码学的作用和地位

什么是密码学？

- 密码学能做什么？
  - 机密性：如何使得某个数据自己能看懂，别人看不懂
  - 认证：如何确保数据的正确来源，如何保证通信实体的真实性
  - 完整性：如何确保数据在传输过程中没有被删改
  - 不可否认性：如何确保用户行为的不可否认性
- 功能如何实现
  - 算法
  - 协议

密码算法

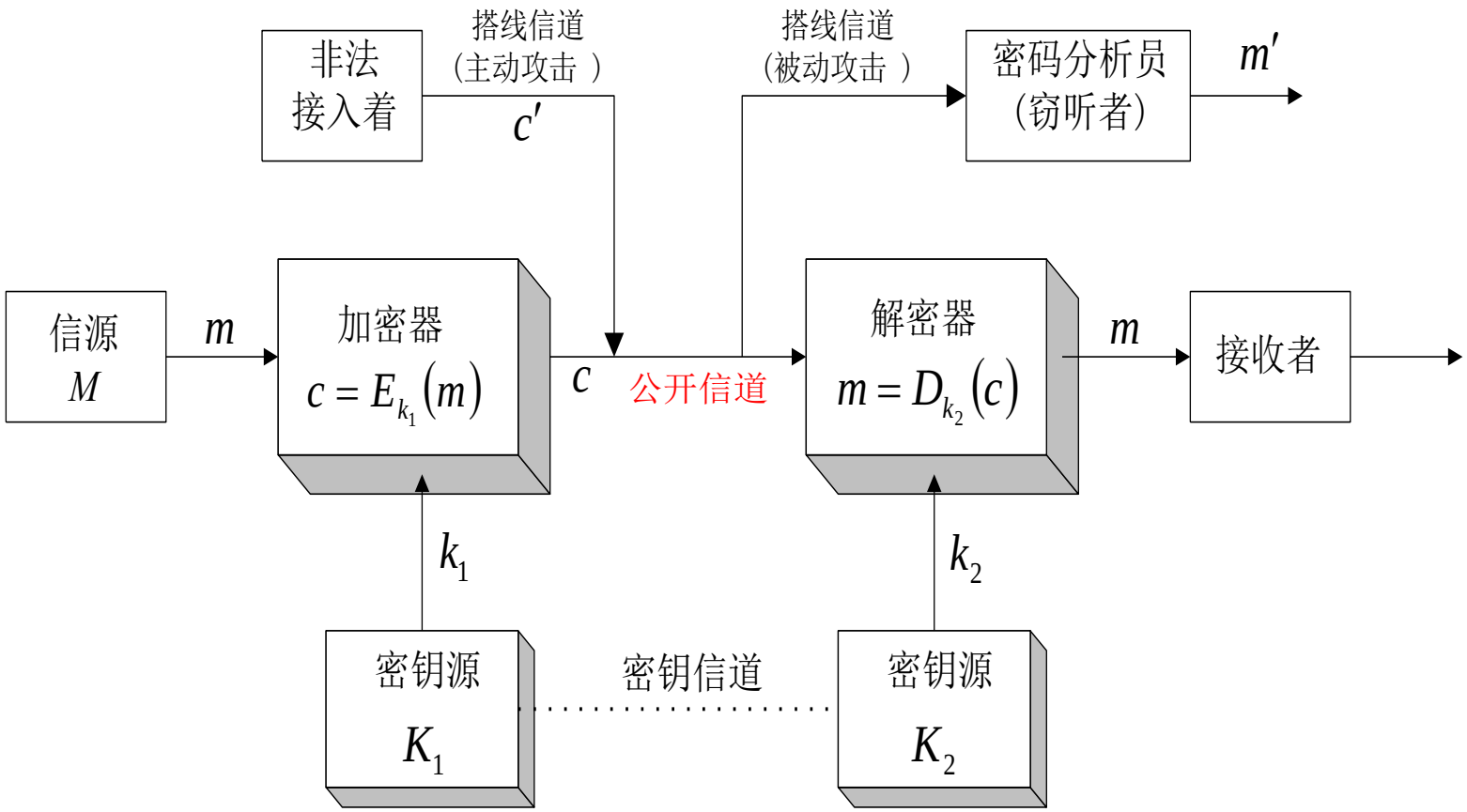
基本概念

- 明文M ——要处理的数据
- 密文C ——处理后的数据
- 密钥k ——秘密参数
- 加密函数：$C = E(k, M)$或$C = E_k(M)$
- 解密函数：$M = D(k, C)$或 $M = D_k(C)$

密码算法（续）

- 密码算法需求：
  - 需求1：可逆——算法的使用者可以将密文恢复成明文
  - 需求2：不可逆——敌手无法将密文恢复成明文
  - 秘密参数——密钥
- 密码算法实际上是一个带有秘密参数的函数。
  - 知道秘密参数，求逆非常容易
  - 不知道秘密参数，求逆是不可行的

保密通信系统模型


非法
接入着
搭线信道
（主动攻击 ）
c'
搭线信道
（被动攻击 ）
密码分析员
（窃听者）
m'
信源
M
m
加密器
$c = E_{k_1}(m)$
c
公开信道
解密器
$m = D_{k_2}(c)$
m
接收者
k_1
k_2
密钥源
K_1
密钥信道
密钥源
K_2

第一讲 密码学的基本概念

- 信息安全的基本属性
- 什么是密码学
- 密码算法的分类
- 密码学的作用和地位

密码算法的分类（续）

按照功能分类

加密算法：用于机密性解决方案

杂凑函数：用于完整性解决方案

数字签名：用于认证和不可否认性

密码算法的分类

按照密钥的使用方式不同分类

对称密钥密码 ：加密密钥与解密密钥相同

如：分组密码，流密码

非对称密钥密码体制:加密密钥与解密密钥不同

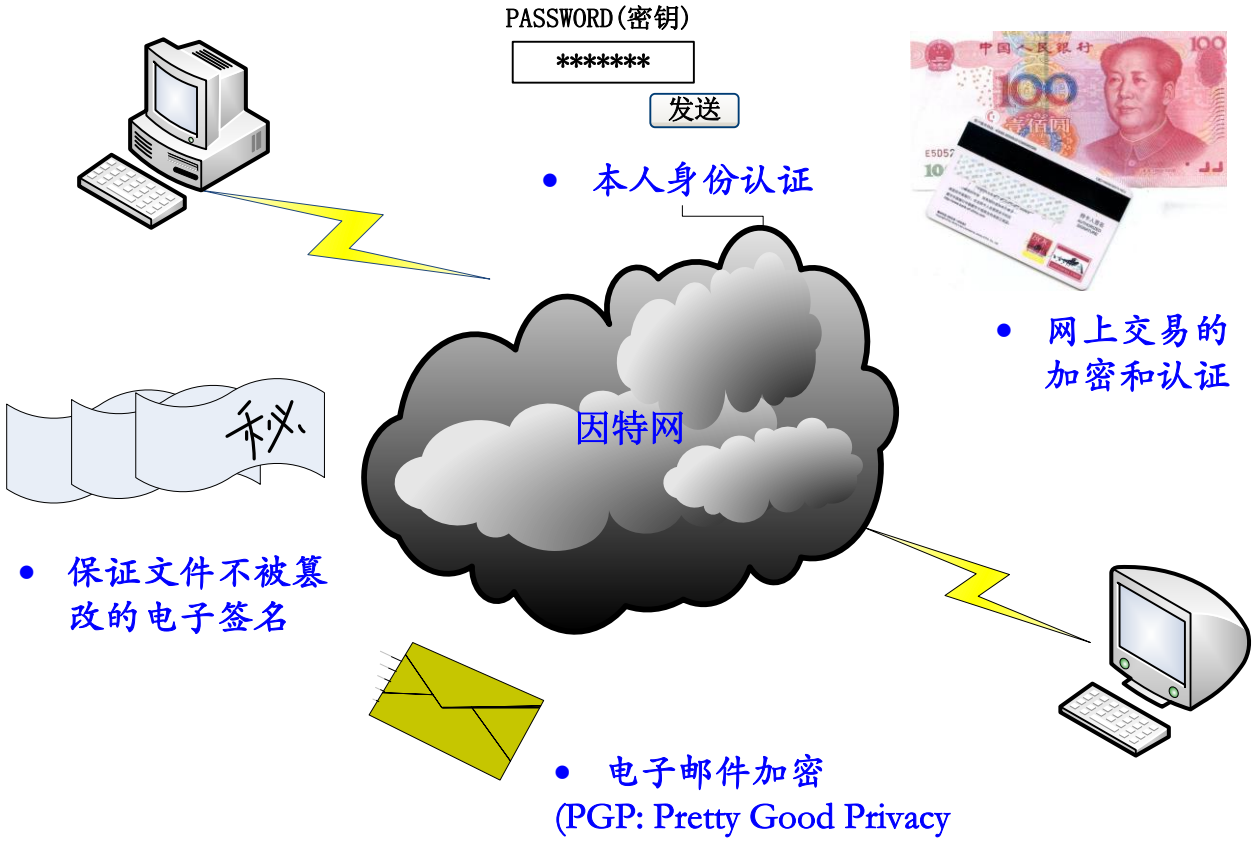
如：公钥加密，数字签名

第一讲 密码学的基本概念

- 信息安全的基本属性
- 什么是密码学
- 密码算法的分类
- 密码学的作用和地位

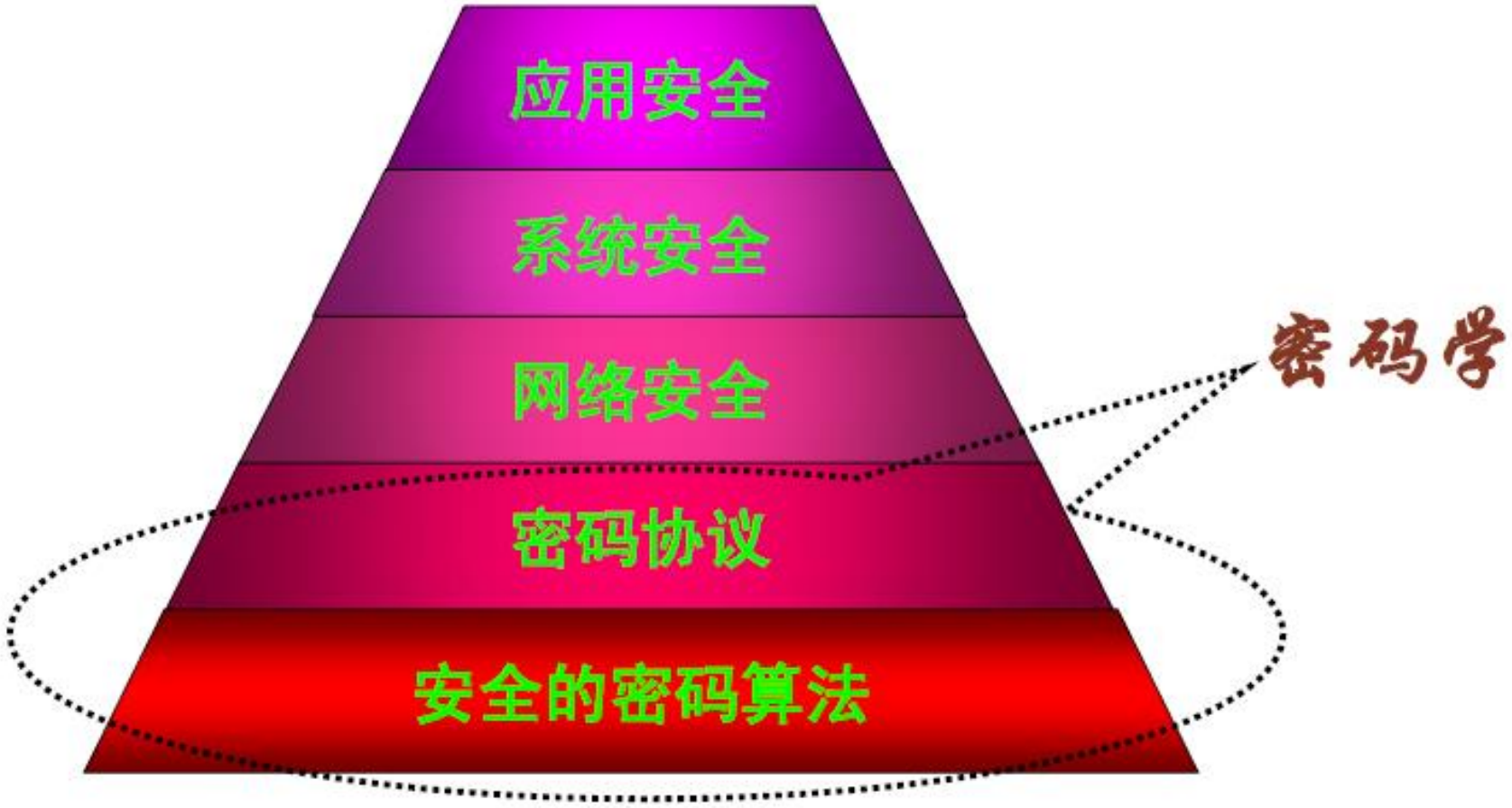
为什么需要密码学？

- **现代密码在社会中的广泛应用**



“密码技术”是保障信息安全的基本技术

密码学在信息安全中的地位



感 谢 聆 听!

xynie@uestc.edu.cn