



第一讲：概述

❖ 无线通信的分类

- 按通信距离划分
- 按应用类型划分
 - 移动通信
 - 无线网络

❖ 信息安全

- 信息安全模型
- 信息安全框架：三个方面
 - 安全攻击常见类型，分类：主动和被动
 - 安全服务的类型及概念
 - 安全机制

❖ 古典密码学

- 古典密码的基本加密方法
- 古典加密的破解方法
- 多表代换密码的概念
 - 维吉尼亚密码

第二讲 密码学

- ❖ 乘积密码概念
- ❖ 对称密钥和非对称密钥的概念
- ❖ 分组加密和流加密的概念
- ❖ Kercheff原则
- ❖ 穷举攻击（暴力破解）的概念
- ❖ 攻击类型
- ❖ 无条件安全和计算安全的概念
- ❖ 混淆和扩散的概念

❖ DES算法

- Feistel架构
- 基本参数：密钥长度，明文长度
- 三重DES

❖ AES算法

- 基本架构
- 基本参数

❖ 工作模式

- 概念
- 五种常见的

❖ 流加密

- 架构
- 需注意的问题

❖ 公钥密码

- 单向函数, 单向陷门函数
- 如何利用公钥密码算法进行加密
- 如何利用公钥密码算法进行认证
- RSA算法
- Diffie-Hellman密码交换协议
- 关于公钥密码学的几点认识
- 关于公钥密码学 and 对称密码学的比较
 - 三个问题

❖ 密钥管理

- 范围
- 密钥分配的方法: 理解
- 基于公钥算法的密钥分配
 - 公钥的分配问题
 - 公钥机构和公钥证书的概念
 - 使用公钥加密分配对称密码体制的密钥

❖ 消息认证

- 消息认证的概念, 和数字签名的区别
- 利用校验和进行消息认证的方法: 两种方式, 一个安全一个不安全
- 消息认证码的定义
 - 消息认证码生成函数与加密函数的区别
- 攻击者攻击的目标
- 如何利用消息认证码进行消息认证

❖ 散列函数

- 基本概念
- 利用散列函数构造MAC码的方法
- 设计要求
 - 弱抗碰撞性
 - 强抗碰撞性

❖ 数字签名

- 基本概念
- 数字签名的常见方法

❖ 公钥证书

- 基本概念
- 公钥证书的产生过程及验证方法

❖ 身份认证

- 认证方式: 单向、双向
- 认证协议的安全目标
- 重发攻击的概念及如何抗重发攻击的常见方法

第三讲

- ❖ 隐藏终端和暴露终端
- ❖ 频分和时分的概念
- ❖ 蜂窝架构
- ❖ GSM系统架构
- ❖ GSM系统的编号
 - MSISDN
 - IMSI
 - TMSI
 - IMEI
 - MSRN
 - LMSI
 - LAI
 - CI
 - BSIC

第四讲

- ❖ 无线局域网的概念
 - 组成
 - AD-HOC模式和Infrastructure模式
 - IBSS、BSS、DS、ESS的概念
 - 无线局域网的接入过程

第五讲

- ❖ GSM的身份认证流程
 - 三元组概念
 - 安全参数和算法分布
- ❖ GSM的匿名保护
- ❖ GSM安全机制存在的问题
- ❖ 3GPP的身份认证
 - 五元组概念

第六讲

- ❖ WEP的认证流程及安全问题
- ❖ WEP加密机制流程
- ❖ WEP加密机制安全问题
 - 数据篡改
 - 初始向量空间太小问题
 - FMS攻击：弱IV问题
- ❖ TKIP协议
 - 针对的WEP安全问题及相应的改进对策
- ❖ CCMP加密机制