目录

一. 信息安全基本概念

二. 信息加密

        - 多字母替代密码
    - 一次一密方案 OTP
        - Verman 密码
    - 转轮机
- 密码学
    - 序列密码（流密码）
    - 分组密码（块密码）
    - Feistel 网络
        - DES 加密算法
        - DES 工作模式
            - 电子密码本 ECB
            - 密码分组链接 CBC
            - 密码反馈 CFB
            - 输出反馈 OFB
- 公钥密码体制
    - 算法条件
    - 单向陷门函数
    - RSA 算法

三. 消息鉴别

- 基于消息摘要的消息鉴别
- 基于 MAC 的鉴别方法
- MAC 函数的设计要点
- 单向散列函数（哈希）
    - MD5 算法

四. 数字签名

- 数字签名的特性
    - 不可伪造性
    - 可信性
    - 不可更改性
    - 不可重用性
    - 抗抵赖性
- RSA 签名体制
- DSS 签名标准
    - DSA 签名算法
- 其他签名模式
    - 不可否认签名
    - 盲签名
    - 群签名
    - 代理签名
    - 指定证实人签名

五. 信息隐藏

- 信息隐藏分类

        - 源路由选择欺骗
    - 网络监听的检测方法
    - 网络监听的防范方法
- 拒绝服务攻击
    - 拒绝服务攻击 DoS
        - SYN 泛洪
        - UDP 泛洪
        - Ping 泛洪
        - 泪滴攻击（碎片攻击）
        - Land 攻击
        - Smurf 攻击
    - 分布式拒绝服务攻击 DDoS
    - 拒绝服务攻击的防范方法
        - 主机设置
        - 网络设备设置
- 缓冲区溢出攻击
- SQL 注入攻击
- 计算机病毒
    - 主控模块
        - 感染模块
        - 触发模块
        - 破坏模块
    - 检测方法
- 木马程序

八. 防火墙

- 性能指标
- 优缺点
- 防火墙技术
    - 包过滤
    - 应用代理
    - 状态检测
    - 地址翻译 NAT
- 防火墙体系结构
    - 屏蔽路由器
    - 单宿主机网关
    - 双宿主机网关
    - 屏蔽子网网关

九. 入侵检测

- 入侵检测系统 IDS
- 入侵检测需求特性
    - 实时性要求
    - 可扩展性要求
    - 适应性要求

十. 身份认证

十一. 区块链