密码技术学习——密码学课程PPT复习提纲

 发表于 2019-06-15 |  分类于 [编程](https://www.edwardzcn98yx.com/categories/%E7%BC%96%E7%A8%8B/)， [密码技术](https://www.edwardzcn98yx.com/categories/%E7%BC%96%E7%A8%8B/%E5%AF%86%E7%A0%81%E6%8A%80%E6%9C%AF/)

 字数统计: 1,123 |  阅读时长 ≈ 4

**CSU密码学课程独门复习提纲**

易考点，并不是“真正意义上”密码学的重点（页数P是按4张PPT一页来的）。

**第一部分 引言**

1. P4 信息安全定义（Information Security）
2. P4 密码学定义（Cryptography）
3. 五类安全服务（认证鉴别服务、访问控制服务、数据保密性服务、数据完整性服务、抗否认服务）（又名：进不来、拿不走、看不懂、改不了、跑不了）
4. P7 安全服务与密码技术的关系（表格）。

**第二部分 密码学概述（古典密码）**

1. P9 理论安全与时间全（香农信息论，资源与运算力限制）
2. P9 四种基本攻击类型
3. P10 对称密码与公钥密码各自的特点
4. P12 几个同余式的定理（运算性质）
5. P16 仿射密码的攻击
6. **P17 维吉尼亚密码特征（弱点、攻击方式）**

**第三部分 现代密码算法**

**数学基础**

1. P21 当p为素数时候，模p的简化剩余系是一个交换乘群。
2. **P22 模、剩余系、完全/简化剩余系的概念**
3. **P23 欧拉函数、欧拉定理、费马小定理**
4. P24 阶、原根定义（利用原根的阶简化计算）
5. P24 原根是否存在的充要条件  其中，p为素数
6. **P25 快速指数算法**
7. **P27 置换群、完美洗牌（从2开始交叉插入）**

**对称密码算法**

1. **P33 DES和IDEA比较（分组位数、轮数、子密个数等）**
2. **P34 P38 AES总结（分组位数、轮数、子密钥个数等）**
3. P39 序列密码与分组密码对比（加密方式）
4. **P47 Hash函数性质**
5. P47 MD5与SHA函数对比
6. **P48经典对称密码算法的特点**

**公钥密码算法**

1. P49 公钥密码算法概述
2. **P50 BSGS算法求离散对数问题，一次同余方程求解**
3. **P51 CRT**
4. P52 二次同余方程、二次符号定理、性质
5. **P53 二次互反定理（**p,qp,q**均为素数的时候判定二次同余方程是否有解加快速度）**
6. P55 P56 素数生成与素性检测算法
7. P57 RSA算法（算法描述、攻击方法、中间人、共模攻击）
8. P60 EIGamal算法（选取k的好处、同密文、发送者多次发送不冲突，对比RSA）
9. P61 ECC算法
10. P62 背包算法（超递增背包->普通背包 加密）
11. **P63 公钥密码算法各种比较**

**签名算法（这里分类有点迷）**

1. P65 RSA签名（密钥使用不当，攻击方式）
2. **P66 DSA算法**
3. **P67 左上签名算法小结**

**第四部分 基本密码协议**

1. P68 密码协议分类（仲裁者裁决者分别对应？？）
2. P70 保密通信协议（公钥密码的中间人攻击、改进方法）
3. P73 密钥协商协议（对称+仲裁者、公钥、DH的中间人、EKE的优势（两者结合）、椭圆曲线DH、双线性对）
4. **P73 密钥协商协议总结**
5. **P78 数字签名协议形式化描述（对称、公钥）**
6. P79 阈下信道
7. P81 身份鉴别协议（SKEY协议单向链、双向鉴别）
8. P83 秘密共享协议（门限分案、Shamir、Bloom）

**第五部分 中级密码协议**

1. **P88 Shamir三次传输协议（异或的问题，不需要共享密钥）**
2. **P88 不经意传输协议（利用上面的、选哪个不知道系列）**
3. P88 （不考）智力扑克协议
4. P89 安全多方计算举例子，理解，盲因子
5. P92 密钥分发协议（加入/不加入会话密钥）
6. P93 基于CRT密钥分发协议+**总结**

**第六部分 高级密码协议**

懂概念、小题

1. P94 **零知识协议目的**
2. P95 盲签名协议（理解）
3. P95 同时签约协议（应用不经意传输，理解）
4. P97 匿名投票协议图示（可能考）+匿名通信协议（不考）
5. P99 数字现金协议图示（理解）

**第七部分 分组密码加密模式**

融入其中了，要考可能只靠特点

1. P103 四种模式总结表格

**第八部分 密钥管理**

1. P105 P106 密钥生命周期内：生成与密钥更新（安全性、哈希生成新密钥）
2. **P106 P107 Kerberos最后一节课特别强调**
3. P108 数字证书概述