密码学

- **基础**
  - 五元组
    - 明文
    - 密文
    - 加密算法
    - 解密算法
    - 密钥
  - 真实性=认证性
  - 主动攻击
    - 中断
    - 篡改
    - 伪造
  - 安全业务
    - 保密业务
    - 认证业务
    - 完整性业务
    - 不可否认业务
    - 访问控制
  - 保密系统的要求
    - 系统即使达不到理论上不可破，也应当为实际上不可破的
    - 系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥-Kerckhoff原则
    - 加密和解密算法适用于密钥空间中的所有元素
    - 系统便于实现和使用
  - 攻击类型
    - 唯密文攻击
    - 已知明文攻击
    - 选择明文攻击 — 选择明文得到密文
    - 选择密文攻击 — 选择密文得到明文
  - 古典密码
    - 凯撒密码 — 后移三位
    - 维吉尼亚密码
      - 根据周期循环密钥之后再移位
      - 本质上仍是移位代换密码
    - 移位变换
      - c=m+k(mod26)
      - m=c-k(mod26)
    - 仿射变换
      - c=am+b(mod26)
      - m=a逆*(c-b)(mod26)
    - 多表代换
      - C=AM+B(modN)
        - 其中A是矩阵
        - N代表字母个数
      - M=A逆*(C-B)(modN)
    - Hill密码
      - 1️⃣看给定的密钥矩阵是几阶的，这里假设3阶
      - 2️⃣将明文消息分割为若干组长度为n的小组，这里n同上假设3
      - 3️⃣将密钥矩阵和明文相乘，结果即密文

- 香农
  - 《保密系统的通信理论》为密码学奠定理论基础
  - 建议密码设计的基本方法
    - 混淆
    - 扩散
    - 迭代
- Diffie+Hellman — 《密码学的新方向》中提出公开密钥思想
- 数论 — 群是一个代数系统
  - 封闭性 — a,b属于G，a·b也属于G
  - 单位元结合律 — a·b·c=(a·b)·c=a·(b·c)
  - 逆元 — 若有a·1=1·a=a，存在a·a逆=a逆·a=1
  - 交换群 — a·b=b·a
- 古典密码实现的两种基本方法
  - 代换
  - 置换
  - （现仍是构造现代对称分组密码的核心方式）

- **对称密码体制**
  - 流密码
    - 线性反馈移位寄存器LFSR
      - 输出序列的表示
      - m序列的判定 — 常见的4级不可规约多项式
        - x4+x+1
        - x4+x3+1
      - LFSR特征多项式与序列的转化
      - m序列伪随机性 — 关于游程的性质
      - m序列的破译 — 根据密钥流和级数得到递推序列
    - 流密码强度完全依赖于密钥流产生器所生成序列的随机性和不可预测性
    - 核心问题是密钥流生成器的设计
    - 分类
      - 同步流密码 — 密钥与明文无关
      - 自同步流密码 — 密钥与明文有关
    - m序列的伪随机性
      - 游程
      - 自相关函数公式P22
      - Golomb随机性公设
        - 在序列的一个周期内
          - 0与1的个数相差至多为1
          - 长为i的游程占总游程的1/(2^i)
        - 异自相关函数是一个常数
      - n长的m序列性质
        - 一个周期内
          - 0个数为2^(n-1)-1,1个数为2^(n-1)
          - 总游程数2^(n-1)，长为i的游程有2^(n-i-1),且0、1游程各半；长为n-1和n的游程为1
        - 自相关函数公式P22
    - m序列的破译
      - 密钥流和密码用矩阵相乘
      - 破解n个寄存器的m序列需要2n个连续的密钥流
  - 分组密码
    - 设计准则
      - 安全性
      - 简洁性
      - 有效性
      - 透明性和灵活性
      - 加解密相似性
    - 设计技巧
      - 计算部件
      - 计算部件的组合
      - SPN（替换/置换网络）
      - 多轮迭代和轮函数
    - 混淆和扩散
      - 混淆性 — 所设计的密码应使得明文、密文、密钥之间的依赖关系相当复杂，以至于这种依赖关系对密码分析者来说是无法利用的
      - 扩散性
        - 所设计的密码应使得密钥的每一个比特影响密文的每一个比特，防止对密钥进行逐段破译
        - 明文的每一个比特影响密文的每一个比特，以便最充分地隐蔽明文
    - Feistel结构 — 结构图记忆
    - DES
      - 基础描述
        - 分组长度64bit
        - 密钥长度56bit（8bit校验位）
        - 16轮变换
      - 初始置换
        - 刚开始进行初始置换
        - 结束进行逆初始置换
      - 轮结构
        - 扩展（E表）将32bit分组变为48bit
        - 密钥左循环移位后也扩展置换，从28bit到48bit
        - 48bit分组和密钥异或后进入S盒代换
        - S盒代换，从48比特到32bit — 8个S盒，输入6bit，输出4bit
          - 第一位和最后一位组合代表行
          - 中间四位代表列
        - 置换（P）
      - 密钥产生
        - 56bit密钥先进行一个置换
        - 分成左右两个部分 均为28bit
        - 左循环移位后进行置换（扩展密钥）
    - 3DES
      - 加密-解密-加密（EDE）
      - 使得已知明文攻击的代价增加到2^112
    - 运行模式
      - ECB电码本模式
      - CBC密码分组链接模式
      - CFB密码反馈模式 — 有错误传播，除保密性外还能用于认证
      - OFB输出反馈模式 — 无错误传播，适用于有扰信道信息传输
      - CTR计数器模式 — 可以产生随机数序列
      - （具体结构图和优缺点见P47）
      - （CBC和CFB的区别见第三章讲义(word)）
    - AES
      - Rijndael
        - 分组和密钥长度均可以为128/192/256bit
        - 不同于DES以比特为单位，该算法以字节为单位进行处理
        - 状态、种子密钥、轮数
          - 不同的Nb和Nk有不同的状态
          - 迭代轮数需要查表
        - 轮函数
          - 字节代换ByteSub
            - 利用S盒实现非线性变换
            - 对字节进行操作代换
            - 字节高四位表示S盒的行，低四位表示列
          - 行移位ShiftRow — 查表得到不同的移位量
          - 列混合MixColumn — 将列与一个固定矩阵相乘
          - 密钥加AddRoundKey
            - 简单地将密钥和状态逐比特异或
            - 轮密钥长度和分组长度相同
            - 轮密钥由种子密钥通过密钥编排算法得到
        - 密钥编排 — 密钥扩展
          - 当Nk<=6时
            - 如果i是Nk的倍数
              - 先将W[i-1]循环移位
              - 再经过一个S盒
              - 将过S盒后的结果和常数Rcon[i/Nk]异或
              - 最后W[i]=上述结果与W[i-Nk]异或
            - 若果i不是Nk倍数 — W[i]=W[i-1]异或W[i-Nk]
          - 当Nk>6时 — 过程与上面的一样，不过有一个特殊情况。就是当i对Nk取模后为4时需要进行一次S盒
        - 密钥的比特数=明文分组长度*(轮数+1)<原因见AES的算法流程图：可发现多了一次轮密钥加少了一次列混淆>
      - Rijndael数学基础 — 在GF(2^8)上
        - 加法 — 将16进制转化为2进制后再转化为多项式，两式相加后取模即可 — 注：取模指取一个不可约多项式，并且该域下也有模2加的性质
        - 乘法 — 步骤同上，不过是多项式的乘法之后再取模 — 例子就看书本P59和期末题
        - 模数为x8+x4+x3+x+1
      - AES其实是Rijndael的一个特殊情况
        - 此时分组长度只能为128bit
        - 密钥可以为128/192、256bit
      - 层数
        - 线性混合层
          - 行移位
          - 列混淆
        - 非线性层 — 字节代换(S盒)
        - 密钥加层

- LFSR中
  - 移位寄存器中存储器的个数=移位寄存器的阶数
  - 移位寄存器中存储的数据=移位寄存器的状态
- 流密码和分组密码
  - 分组密码与流密码的区别就在于有无记忆性
  - 流密码又叫单字母/单码代换
  - 分组密码又叫多字母/多码代换
- 单钥密码体制不仅可用来加密，还可用来认证
- 扩散性的理解
  - 粘连性 — 明文、密文、密钥的每一位都相互依赖
  - 不连续性/雪崩性 — 当改变明文的任何一个比特时，对应密文改变的比特个数是一个随机变量
  - 不可部分破译性 — 分组密码不能分解成若干子密码。对分组密码的攻击要么彻底破解，要么一无所获
- 若DES加密第一轮用k1，则16轮后解密第一轮用k16
- 如果某一组明文/密文对（m，c）使得方程m=D（c，z）特别容易解出z，m就称为一个弱明文，z就称为一个弱密钥
- DES普通的CBC模式和CBC-MAC的区别 — 普通的CBC模式中要对第一个明文使用初始向量IV异或后再加密处理

- **公钥密码体制**
  - 数论
    - 阶Ord_m(n) — 等于n^qmodm=1时的q值
    - 欧拉函数fai(n)
      - 为素数时 — 素数-1
      - 不为素数时 — 分解为素数的乘积后为n*(1-1/a)*(1-1/b)…(…)
      - 分解为两个素数相乘时 — 两素数-1后相乘
    - 快速模幂
  - RSA
    - 定理
    - 性质
    - 解密过程
      - m与n互素
      - m与n不互素
    - 攻击
      - 共模攻击
      - 低指数攻击
  - 椭圆曲线密码体制 — 椭圆曲线
    - 关于x轴对称，是一个y方和x三方的方程
    - 加法律
      - P+O=P
      - P1(x,y)的加法逆元为P2=-P1=(x,-y)
      - 三个点在一条直线上则加法合为0，即P+Q+P1=0
    - E_p(a, b)=x^3+ax+b(mod p)
    - 计算P(x1,y1)+Q(x2,y2)=(x3,y3)
      - 入=
        - P!=Q时 — (y2-y1)/(x2-x1) — 直线
        - P=Q时 — (3*x1^2+a)/(2*y1) — 利用导数式子来记忆
      - x3=入^2-x1-x2(mod p)
      - x4=入(x1-x3)-y1(mod p)
      - 其中关于入计算中所有的除法都是乘逆元！！！但上下两个可约分，这个可以方便运算！
  - 困难问题
    - FAC大整数分解
    - DLP离散对数
    - ECC椭圆曲线

- **哈希函数（散列、杂凑函数）**
  - 基本满足条件
    - 任意长输入、固定长输出
    - 抗原象性
    - 抗弱碰撞性
    - 抗强碰撞性
  - MD5
    - 任意长度输入
    - 512bit的分组来进行处理
    - 128bit输出
    - 4轮
    - 过程
      - 1.消息填充 — 使得其比特长在模512下为448（这一步是必须的）
      - 2.附加消息的长度 — 留出的64bit以小端方式来表示消息被填充前的长度
      - 3.对MD缓冲区初始化 — 4个缓冲区表示为4个32bit长的寄存器
      - 4.以分组为单位对消息进行处理
      - 5.输出
  - SHA1
    - 小于2^64bit长的任意消息
    - 160bit输出
    - 过程
      - 1.消息填充（和MD5一样）
      - 2.附加消息的长度 — 大端方式
      - 3.对MD缓冲区初始化 — 5个32bit长的寄存器
      - 4.以分组为单位对消息进行处理
      - 5.输出
  - 消息认证码MAC
    - 使用一个密钥来进行计算校验和
    - 实现了认证性(真实性)、完整性
    - 时间性、顺序性
  - HMAC
    - 典型应用在"挑战/响应"中，用于对身份进行认证
    - 哈希函数与密钥的结合
  - （两者安全性的比较P174）

- 盲签名 — 特点
  - 签名者不知道自己签署信息的内容
  - 签名消息不可追踪

- **数字签名**
  - 性质
    - 完整性
    - 身份唯一性
    - 不可否认性
  - 签名方案
    - RSA
    - ELGamal
    - DSA
    - （基于离散对数）

- **安全协议**
  - 对称密钥的密钥分发
    - 密钥分配中心KDC（P136）
      - 五个过程
      - 两个随机数
        - 都是通过挑战应答来验证身份
        - N1验证KDC、N2验证B
    - 密钥的控制使用
      - 根据用途分为会话密钥、主密钥
        - 会话密钥-数据加密密钥
        - 主密钥-密钥加密密钥
      - 主密钥安全性应高于会话密钥
  - 非对称的密钥分发
    - 公钥的分配
      - 公开发布 — 任何人都可伪造
      - 公用目录表 — 由可信实体/组织承担，但管理员的秘密钥被获取后就gg
      - 公钥管理机构 — 管理机构可能成为系统的瓶颈
      - 公钥证书 — 由证书管理机构CA建立，CA用自己的私钥签名形成证书
    - 利用公钥加密体制来分配
      - 简单分配 — 易收到中间人攻击
      - 保密性和认证性的密钥分配P143 — 类似三次握手后签名发送密钥
      - Diffie-Hellman密钥交换
  - Kerberos
    - 基于对称密钥
    - 防止假冒
    - 三个阶段
      - 认证服务交换 — 用户从AS获取票据许可票据
      - 票据许可服务交换 — 用户从TGS获取服务许可票据
      - 客户机-服务器的认证交换 — 用户从服务器获取服务
    - 认证系统中符号及其意义
      - AS-认证服务器
      - TGS-票据许可服务器
  - X.509
    - 以公钥密码体制和数字签名为基础
    - 发放证书方式：CA<<A>>表示CA向A发放证书
    - 证书不可伪造，有层级，用证书链表述
    - 证书吊销：CA来维护证书吊销列表CRL
    - 认证过程
      - 单向认证 — 证明发送方身份等
      - 双向认证 — 单向基础上证明身份
      - 三向认证 — 检查重放攻击 — 看书本P288/9
    - 为防止公钥盗用而设计
  - PKI — 公钥基础设置 — 核心是CA（认证机构）
  - SSL/TLS
    - 对称密钥通信框架
    - SSL安全套接层
      - 四次握手
        - 建立安全功能
        - 服务器认证与密钥交换
        - 客户端认证与密钥交换
        - 完成
      - 记录协议
        - 保密性
          - 握手协议定义了加密SSL载荷的传统加密共享密钥
          - 握手协议定义了生成消息认证码MAC的共享密钥
        - 消息完整性
    - TLS传输层安全协议 — SSL标准化后的名称
  - IPsec
    - 网络层的安全协议
    - 协议
      - AH
        - 认证的扩展报头
        - 认证，实际应用中不使用
      - ESP
        - 实现加密和认证(可选)的扩展报头
        - 加密，可以认证，主流方法
      - IKE
      - 工作模式
        - 传输模式 — 为上层协议提供保护 — 不会产生新的IP头源地址
        - 隧道模式 — 对整个IP数据报提供保护 — 会产生新的IP源地址
        - 两种模式对于AH、ESP的示意图（见PPT）
    - 策略
      - SA安全关联
      - SAD安全关联数据库
      - SPD安全策略数据库
    - 密钥管理
  - IKE — 基于DH交换

- KDC主要负责密钥的分发和产生
- 注：票据可重复使用且有效期较长；而认证符只能使用一次且有效期很短