对称密码学

密码体制安全性

- 无条件安全性 — 即便是攻击者有无限的计算资源,也无法破译
- 计算安全 — 攻击者在目前或未来已有的计算资源的条件下无法破译
- 攻击者的攻击能力越强,要实现的目标越低,越难对付

对称密码

★ 流密码

- 前言
  - ★ 如何产生随机数
    - 计算机只能产生伪随机数 — John von Neumann
    - 我们需要的 — ★ 密码学意义上安全的伪随机序列
      - ★ 在统计上应该是随机的
      - ★ 不可预测性
      - ★ 不能被可靠的重复产生 — 用完全同样的输入操作两次,得到的是两个不相关的序列
    - 真随机数 — 哲/学问题 — 比如电/流及生器
- ★ 一次一密
  - 加密:明文流与密钥流对应比特异或
  - 解密:密文流与密钥流对应比特异或
  - 密钥流是真随机序列,且不可以重复使用 — 安全性:无条件安全
    - 密钥是真随机的
    - 无条件安全性的概率意义
    - 对于任意概率 p 和概率 K ,都有 $Pr[x \mid y] = Pr[x]$
    - 即,不能通过分析密文获得任何关于明文的信息
  - 然而并没有什么卵用
- 流密码
  - 基本思想
    - 用一个较短的密钥生成密钥流,在攻击者看来是随机的 — 输入一个较短的密钥,产生源源不断的密钥流
      - 密钥又称为种子
    - 不是无条件安全的,只是计算上的安全
  - 同步流密码 — 密钥流自与密钥有关,且需要双方的密钥流生成器初始状态一致
  - 自同步流密码
    - 密钥流还与明文有关
    - 把明文的每个比特扩散到密文的多个比特中
    - 具有有限的差错传播能力
  - 密钥流生成器
    - 驱动部分 — 为非线性部分提供伪随机序列 — ★ FSP反馈移位寄存器
      - 输入密钥
      - 通过反馈函数迭推 — 在每个时刻,各级都有一个值,作为内部状态
        - 在时钟脉冲的控制下,各级的值告向前移动一级
        - 最前面一级作为输入,最后一级的值由 f 的输出填充 — $x_{n+1} = f(x_1, x_2, \ldots, x_n)$
      - 产生一个周期长,线性复杂度高,统计特性好的初始序列
    - 非线性组合部分 — 产生密码学意义上安全的伪随机序列

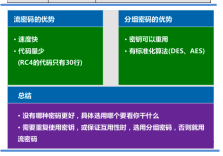
★ 分组密码(分组密码应用极其广泛)

- 设计思想
  - ★ 在密钥的控制下,把 n 比特的明文分组,简单且迅速的置换成唯一的 n 比特的密文分组,且这种变换是可逆的(不然咋解密)
  - 它必须是一个双射函数 — 明文空间等于密文空间
  - ★ 混乱与扩散
    - 对抗攻击者对密码系统的统计分析
    - 混乱 — 使得明文与密文,密文与密钥将的统计特性极小化 — 代换 — 明文2^n,可逆变换 (2^n)!
    - 扩散 — 使得明文及密钥的影响尽可能扩散到较多的密文比特中 — 置换
  - DES数据加密标准
    - 输入输出均为 8 比特的倍数
    - 分组长度:明文密文都是 64 比特 — ★ 明文长度不够时,填充最后一个字节
    - 密钥长度 64 比特
      - 有效密钥 56bit
      - 奇偶校验8bit
    - 加密和解密过程完全相同,子密钥的使用顺序完全相反
    - E盒 — 32bit->48bit
    - ★ S盒
      - 将输入的 48bit 分成 8 组,每组 6bit,输出 4bit,48bit->32bit
      - 唯一的非线性部分
      - 雪崩效应
    - P盒 — 对S1 到 S8 的输出 32bit 进行坐标置换
    - 密钥空间只有 10^17
    - ★ 三重DSE — 使用2/3 个密钥,执行 3 次 DSE
      - 二重DES 存在中间人攻击

★ 应用

应用	所用密码	评价
数据包	AES	与其他软件的互用性不是问题
E-mail	AES	也可用流密码,但考虑到AES要安全普遍用,使用AES可以使你与E-mail服务器保持互用性。
SSL	RC4(流密码)	速度是非常重要的,每次通信需要使用不同的密钥,而且事实上,所有浏览器和服务器都有RC4
文件加密	分组密码	可以用相同的密钥保护不同的文件,密钥管理很方便

★ 对比



五种工作模式

- 电子密码本 ECB — ★ 每个明文分组单独加解密
  - 简单,快
  - 无差错传播
  - 容易被攻击
  - 不推荐
- 密码分组链 CBC — 每个明文分组先与前一密文分组异或,再进行加解密
  - ★ 依赖初始矢量 IV
  - 慢
  - 有限的误差传播
- 密码反馈CFB
  - 每次只取取 此特 — 更慢
  - CFB适用于 明文按字符(如电传电报)或按比特处理的流密码中
- 输出反馈 OFB — 和上一个很像
- 计算器CTR — CTR适用于 需要并行处理的应用领域

对称密钥的管理

- 密钥很难被人记忆(人均记忆大师) — 还是保存密钥比保存明文容易一些
- 基于口令的 PBE — 口令+salt-->hash()
  - salt防止字典攻击
- 基于硬件的密钥存储 — 令牌 — 校园卡
- 保护密钥的密钥 — KEK
- 生物特征 — 指纹解锁

课后题

1. 流密码体制由 (D) 两部分组成

A. 驱动部分、反馈函数　　B. FSR、反馈函数

C. FSR、非线性组合部分　　D. 驱动部分、非线性组合部分

2. 设计分组密码的两种技术是 (C)

A. 置换和移位　B. 易位和置换

C. 混乱和扩散　D. 隐写和扩散

3. (D) 不是分组密码的工作模式

A. CBC　B. OFB　C. CTR　D. PBE

4.下列哪个不是分组密码体制 (D)

A. DES　B. AES　C. IDEA　D. RC4

5.下列哪种模式的安全性最差 (A)

A. ECB　B. CBC　C. OFB　D. CFB

6. CBC模式中，一个密文分组传输错误，会影响(B)个密文分组的解密

A. 1　B. 2　C. 3　D. 4