2020 CTF暑假夏令营培训Day2 密码学Crypto 部分笔记

原创

小哈里 于 2021-10-09 12:26:19 发布 45 收藏
分类专栏： # 网络安全 文章标签： crypto

本文链接：https://blog.csdn.net/qq_33957603/article/details/120668603

网络安全 专栏收录该内容
19 篇文章 10 订阅
订阅专栏

Day2密码学 - Crypto

架构

- 研究内容有：信息m的加密A、解密B、加密后的信息C（第三方是否可窃取）。
- 密码的分类：古典密码（关注算法的机密性，一般是置换和代换，打乱顺序，变量映射等），现代密码（假设算法大家都知道，关注信息本身的复杂度）
- 序列密码，核心为PRNG（伪随机数生成器）生成伪随机数序列，通过加密函数与明文加密生成密文，解密时生成一样的序列，用逆函数运算。

古典密码

- 历史：斯巴达密码棒，凯撒，维吉尼亚，希尔Hill，山农shannon，公钥ECC，DES，然后RSA，DSA，ECDSA，AES。
- 斯巴达密码棒（缠绕纸打乱。栅栏密码，置换密码只换顺序不换映射）
- 单表替换密码（明文->算法=密文，双方保管共同算法）
  凯撒密码（(明文+3)%26）
  猪圈密码（共济会密码，字母映射为各种符号）
  CTF中那些脑洞大开的编码与加密（与佛论禅，社会主义核心价值观编码，Ook!，Rrainfuck，Jsfuck，云影密码，跳舞的小人，键盘密码等）
  简单替换密码（通过密钥替换，可以统计字母频率解密）
- 多表替换密码
  维吉尼亚（明文+密钥->=密文，横纵坐标替换。破解时发现周期性的偏移量是固定的，转换为多组单表替换。只需要爆破密钥长度即可，此方法为卡斯基检测法。）
  xnuca2018baby（吻合指数，正常文章为0.66，统计字母频率，）

现代密码

- RSA，基于整数分解（
  欧拉函数φ(n)，模n下与n互素的整数个数。
  欧拉定理，若gcd(a,n)==1, 则a^φ(n)%n==1。
  模逆，即该数的逆元，一般用拓展欧几里得求。
  指数，gcd(a,n)==1, 若满足a^e%n==1的最小整数e，即a对%n的指数ord(a), 如果该数==φ(n), 则a称为原根。）。
- RSA，最著名的非对称算法。
  对于需要加密的信息flag，将其以某种形式转化为数字m（m即明文）。
  寻找两个大素数p,q满足n=p*q, n>m，寻找一个整数e，满足gcd(e, φ(n))=1。
  计算e%φ(n)下的逆元d，则有e*d%φ(n)==1。(n, e)作为公钥，d作为私钥。
  加密时，密文c = m^e%n。解密时，明文m=c^d%n。
- 常见套路：n可以直接分解（factordb/yafu进行分解，毕竟rsa无解）。e过小（直接开根）

02:33:45