RSA小扎

原创

端阳月七 于 2021-02-12 09:05:25 发布 1180 收藏
分类专栏： Network Security 文章标签： 数据库 c# asp.net

本文链接：https://blog.csdn.net/h6h26169i10l34fsgrh/article/details/113774128

预备知识

1. a mod b = c: a除以b的余数是c(1除以160的余数是1)；
2. a ≡ b (mod m): 如果两个整数a和b满足a-b能够被m整除，即(a-b)/m得到一个整数，那么就称整数a与b对模m同余;
3. gcd(a, b) = c: a和b都能被c整除(a = mc, b = nc)；
4. 欧拉函数ϕ(n): 整数1 <= a < n中满足gcd(a,n)=1的个数(在比n小的整数里和没有公因数的素数的个数)，ϕ(n) = n(1-1/p1) (1-1/p2)… (1-1/pm);

RSA算法步骤

1. 用户选择两个大的随机素数 p, q；
2. 计算N=p.q ；
3. 计算n的欧拉数： ø(N)=(p-1)(q-1) ；
4. 随机算则一个加密密钥e：1<e<ø(n), gcd(e,ø(n))=1 ；
5. 解以下方程得到解密密钥 d ：e.d=1 mod ø(n) and 0≤d≤n；
6. 加密消息M得到密文 C=Me mod N；
7. 解密密文得到明文 M=Cd mod N；

RSA算法示例

1. 算则两个素数: p=17 & q=11
2. 计算 $n = pq$ =17×11=187
3. 计算 $ø(n)=(p-1)(q-1)$=16×10=160
4. 选择 e：gcd(e,160)=1； 其中e=7
5. 计算d: de=1 mod 160 and d < 160

   d=23 （因为23×7=161= 10×160+1）
6. 公布公钥KU={7,187}
7. 保存私钥KR={23,17,11}

- 如果待加密的消息 $M = 88$ (注意： $88<187$)
- 加密：$C = 88^7 \bmod 187 = 11$
- 解密:$M = 11^{23} \bmod 187 = 88$

easy_RSA

在一次RSA密钥对生成中，假设p=473398607161，q=4511491，e=17.求解出d。

1. Euler Theorem；
2. 模运算：伪随机数、散列算法；
3. RSA：用公钥加密密文后，确保不能根据公钥反推出来，也就是说什么运算反推不容易且单向计算容易呢？

> 参考资料：
>
> 1. 攻防世界-crypto-easy_RSA_南海小鱼干的博客-CSDN博客_easy_rsa；
> 2. 探秘公钥加密算法 RSA_哔哩哔哩_bilibili；
> 3. XCTF-攻防世界-密码学crypto-新手练习区-writeup_Ryannn_的博客-CSDN博客

Normal_RSA

1. Kali；

> 攻防世界-crypto-Normal_RSA（openssl和rsatool工具解密RSA） - zhengna - 博客园