2024/01/24

密码学第二次课程RSA

RSA从入门到退坑

汇　报　人：王添翼

汇报时间：2024/01

FJNU-NISA

目录

1. RSA基础知识概述

算法核心流程

选择两个大素数p和q，计算n=p×q。

计算欧拉函数φ(n)=(p- 1)×(q- 1)。

选择整数e，满足1<e<φ(n)且gcd(e, φ(n))=1，作为公钥。

计算e的模逆元d，满足ed≡1(mod φ(n))，作为私钥。

加密过程：将明文m转换为密文c，计算c=m^e mod n。

解密过程：将密文c转换为明文m，计算m=c^d mod n。

例如，选择p=61，q=53，n=3233，φ(n)=3120，e=17，d=2753。对于明文m=65，加密后密文c=2790，解密后可还原为m=65。

数学基础

素数与互质数：素数是只有1和本身两个因数的正整数，互质数是指两个数的最大公约数为1。在RSA中，p和q是素数，e与φ(n)互质。

模运算与同余：模运算是取余数的运算，如a mod b表示a除以b的余数。同余是指两个整数a和b满足a- b能被m整除，记作a≡b(mod m)。RSA加密和解密过程都基于模运算。

欧拉函数与欧拉定理：欧拉函数φ(n)表示小于等于n的正整数中与n互质的数的个数。欧拉定理指出，若a与n互质，则a^φ(n)≡1(mod n)。这为RSA中计算模逆元提供了理论基础。

安全性原理

RSA的安全性基于大整数分解的困难性。给定两个大素数p和q的乘积n，很难在有限时间内分解出p和q。一旦分解出p和q，就可以计算出 $\phi(n)$，进而求出私钥d，从而破解加密信息。

目前被破解的最长RSA密钥是768位，对于1024位及以上的密钥，破解难度极大。随着计算能力的提升，密钥长度也在不断增加，以确保安全性。

举个小例子

好的这一部分还没写，不过没关系你可以直接通过做题来学习~

2. RSA的攻击手段

直接分解n攻击

费马分解法

当n的两个质因数p和q相差较小时，费马分解法较为有效。该方法利用平方差公式，通过寻找两个平方数之差等于n的方式来分解n。例如，对于n=85，可以找到$9^2 - 4^2 = 85$，从而分解出p=9+4=13，q=9- 4=5。随着计算能力的提升，对于较小的n（如512位以下），费马分解法可能构成威胁。

01

Pollard p-1分解法

该方法基于数论中的性质，适用于n的质因数p- 1具有较小质因数的情况。通过计算一系列数的乘积模n，寻找满足特定条件的数来分解n。例如，对于n=1387，选择合适的基数和指数进行计算，可以分解出p=19，q=73。对于一些特定的RSA密钥，Pollard p- 1分解法可能在较短时间内找到质因数。

02

网站分解工具

一些在线分解工具或网站，如Factordb等，提供了强大的计算资源和优化的算法，可以快速分解较小的n。这些工具通常基于分布式计算和先进的数学算法，对于CTF比赛中的RSA题目，如果n的位数较短，可以尝试使用这些工具进行分解。

03

低加密指数攻击

01

攻击原理

当公钥指数e较小时，如e=3，攻击者可以通过枚举或利用特定数学性质来尝试找到明文m。如果明文m较短，攻击者可以尝试对密文c进行开e次方根运算，得到一个接近m的值。例如，对于密文c=12345，公钥(n,e)=(3233,3)，攻击者可以尝试计算iroot(c,e)，如果结果为整数，则可能得到明文。

02

攻击实例

在BUUCTF的Dangerous RSA题目中，公钥指数e=3，攻击者通过枚举k值，计算c+k×n的e次方根，最终找到明文。这种方法在e较小且明文较短时较为有效，CTF选手需要熟悉这种攻击方式，并在遇到类似题目时快速尝试。

共模攻击

攻击原理

当两个不同的明文m1和m2使用相同的模数n和不同的公钥指数e1和e2进行加密时，攻击者可以利用扩展欧几里得算法找到一组整数s1和s2，使得$s1 \times e1+s2 \times e2 \equiv 1 (\mod \Phi(n))$。然后通过计算c1^s1×c2^s2 mod n，可以得到明文m1或m2。这种攻击利用了模运算的性质，对密钥管理不当的情况较为有效。

攻击实例

在BUUCTF的BJDCTF2020 rsa_output题目中，攻击者通过共模攻击成功解密出明文。题目给出了两组密文和公钥指数，攻击者利用共模攻击的原理，计算出明文。这种攻击方式在CTF比赛中较为常见，选手需要掌握其原理和实现方法。

公因数攻击

攻击原理

当多个密文使用相同的模数n和不同的公钥指数进行加密时，如果这些密文之间存在公因数，攻击者可以通过计算最大公约数（GCD）来找到公因数，从而破解部分密文。例如，对于两个密文c1和c2，如果gcd(c1,c2)=k，那么可以利用k来解密其中一个密文。

攻击实例

在BUUCTF的RSA5题目中，攻击者通过公因数攻击成功解密出部分密文。题目给出了多组密文和公钥指数，攻击者利用公因数攻击的原理，计算出公因数，进而解密出部分明文。这种攻击方式在CTF比赛中较为常见，选手需要掌握其原理和实现方法。

低解密指数攻击（Wiener攻击）

攻击原理

当私钥d较小时，攻击者可以通过Wiener攻击来破解RSA。Wiener攻击基于连分数展开，将公钥指数e和模数n表示为连分数的形式，通过寻找合适的渐进分数来近似表示d/φ(n)，从而得到私钥d。这种方法在d较小或e较大时较为有效。

攻击实例

在BUUCTF的RSA2题目中，攻击者通过Wiener攻击成功破解了RSA加密。题目给出了公钥(n,e)，攻击者利用Wiener攻击的原理，计算出私钥d，进而解密出明文。这种攻击方式需要选手掌握连分数展开和Wiener攻击的具体实现方法。

PART 03

RSA安全性提升措施

POWERPOINT DESIGN

这里还没写（光速逃）
不过这里并不是CTF比赛的重点（毕竟awd(p)赛程中没有密码学，无需加固）
但是这个思想还是挺重要的（确信）
相信你会随着一步步的做题，感悟逐渐增多的（确确信）


谢谢观看