RSA 攻击

丁湛钊

1901210628

January 4, 2020

Overview

1. RSA 回顾
2. 几种攻击

RSA 体系

- 欧拉定理：$a^{\phi(N)} \equiv 1 \ (mod \ N)$，也就是 $a^{\phi(N)} = kN + 1$
- 密钥生成
  - 选择两个素数 p 和 q
  - 生成模数 $N = pq$，计算 N 的欧拉函数值 $\phi(N) = (p-1)(q-1)$
  - 选择任意公钥指数 e 使得 $1 < e < (p-1)(q-1)$，另外 $gcd(e, (p-1)(q-1)) = 1$，此时 e 和 N 作为公钥
  - 计算私钥 $d = e^{-1} \ (mod \ (p-1)(q-1))$
- 加密过程: $c = m^e$
- 解密过程
  - $c^d = m^{ed}$
  - $ed = 1 \ (\ mod \ \phi(N)), ed = 1 + k\phi(N)$
  - $m^{ed} = m^{1+k\phi(N)} = m^1 \times (m^{\phi(N)})^k = m \ (mod \ N)$

共模数攻击 Common Modulus Attack

- 贝祖定理：当 $ax + by = m$ 中的 x 和 y 有整数解时，m 是 $gcd(a, b)$ 倍数
- 计算过程：扩展欧几里得

共模数攻击 Common Modulus Attack

- 对 N 的攻击
- 前提
  - N 被用于重复加密
  - e 不同，且当 $i \neq j, gcd(e_i, e_j) = 1$
- 示例
  - 第一次：$c_1 = m^{e_1} \pmod N$
  - 第二次：$c_2 = m^{e_2} \pmod N$
  - $gcd(e_1, e_2) = 1$
- 攻击过程
  - $e_1 x + e_2 y = gcd(e_1, e_2) = 1$ 有整数解（贝祖定理，扩展欧几里得计算）
  - $c_1^x \times c_2^y = (m^{e_1})^x \times (m^{e_2})^y = m^{e_1 x} \times m^{e_2 y} = m^{e_1 x + e_2 y} = m^1 = m$

费马分解攻击 Fermat Factoring Attack

- RSA 中使用 p 和 q 生成模数 N，如果可以恢复出 p 和 q 则被攻破
- 前提：$|p-q| < \sqrt[4]{N}$
- 攻击思路
  - $\frac{(p+q)^2}{4} - N = \frac{(p+q)^2}{4} - pq = \frac{p^2+2pq+q^2-4pq}{4} = \frac{(p-q)^2}{4}$
  - 由于 $|p-q|$ 比较小，所以 $\frac{(p-q)^2}{4}$ 比较小，所以 $\frac{(p+q)^2}{4}$ 和 N 比较接近
  - 所以 $\sqrt{N}$ 和 $\sqrt{\frac{(p+q)^2}{4}} = \frac{(p+q)}{2}$ 比较接近
  - N 已知，可以通过在 $\sqrt{N}$ 的附近找到 $\frac{(p+q)}{2}$
  - 确认是不是 $\frac{p+q}{2}$ 的方法：当前的数为 x，查看 $x^2 - N$ 是否为平方数
  - 当 $x = \frac{p+q}{2}$ 时，$x^2 - N = \frac{(p-q)^2}{4} = (\frac{p-q}{2})^2$

Hastard 广播攻击 Hastard Broadcast Attack

- RSA 中使用了公开指数 e
- 前提： e 比较小，且未使用复杂的填充方案， $m < N_i$
- 示例 $e = 3$
  - $c_1 = m^3 \pmod{N_1}$
  - $c_2 = m^3 \pmod{N_2}$
  - $c_3 = m^3 \pmod{N_3}$
- 中国剩余定理
  - $$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$
  - 解： $x = \sum a_i t_i M_i \; (\bmod M)$ 其中 $M = \prod m_i, M_i = \frac{M}{m_i}, t_i M_i \equiv 1 \pmod{m_i}$

Hastard 广播攻击 Hastard Broadcast Attack

- 攻击思路：
  - $m < N_i$ 所以 $m^3 < N_1 N_2 N_3$
  - 使用中国剩余定理得到 $m^3 = c \pmod{N_1 N_2 N_3}$
  - 此时 m^3 可以直接开方
  - 当 e 更大的时候，使用更多的等式就可以做到同样的效果
- 避免攻击
  - 使用更大的 e： 增加难度
  - 使用复杂的带有随机性的填充方案：使得广播时的 m^n 不相同

Wiener 攻击 Wiener's Attack

- 连分数：形如 $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$ 的分数，其中 a_i 为整数，表示为 $[a_0; a_1, \dots, a_n]$
- 定理：任意有理数都可以被写为有限个连分数的形式
- 计算方法：欧几里得算法，计算 $\frac{x}{y}$ 对应的连分数表示形式可以通过计算 $gcd(x, y)$ ，其中的商部分即为 a_i
- 渐近分数：只取连分数中的前 x 个（$x < n$）
- 举例：$\frac{12}{5}$
  - $2 + \frac{1}{2 + \frac{1}{2}}$
  - 表示为：$[2; 2, 1]$
  - 渐近分数：$2, 2 + \frac{1}{2} = \frac{5}{2}$
- 定理：$|\frac{a}{b} - x| < \frac{1}{b^2}$ 则 $\frac{a}{b}$ 是 x 连分数展开的渐近分数之一

Wiener 攻击 Wiener's Attack

- 在 RSA 中，如果私钥 d 过小可能存在问题
- 前提： $d < \frac{1}{3}N^{\frac{1}{4}}$
- 攻击思路：
  - $ed = 1 \ (mod \ (p-1)(q-1))$ 所以
    $ed = 1 + k(pq - p - q + 1) = 1 + k(N - p - q + 1)$
  - $$\begin{aligned} \left|\frac{e}{N} - \frac{k}{d}\right| &= \left|\frac{ed}{dN} - \frac{kN}{dN}\right| \\ &= \left|\frac{1 + kN - k(p+q-1)}{dN} - \frac{kN}{dN}\right| \\ &= \left|\frac{1 - k(p+q-1)}{dN}\right| \leq \left|\frac{3k\sqrt{N}}{dN}\right| < \frac{1}{2d^2} \end{aligned}$$
  - 由连分数中的定理： $\frac{k}{d}$ 是 $\frac{e}{N}$ 的渐近分数之一

Wiener 攻击 Wiener's Attack

- 攻击思路：
  - $\frac{ed}{k} = e \times \frac{d}{k} = \frac{1+k(N-p-q+1)}{k} = \frac{1}{k} + N - (p+q) - 1$
  - 此时，对 $\frac{e}{N}$ 的渐近分数进行遍历，可以得到 $p+q$ 的可能值
  - 求解方程 $x^2 - (p+q)x + pq = 0$ 的解，如果有整数解，说明分解成功

近年发展

现有方法的进一步提高:

- K. Somsuk, K. Tientanopajai, An improvement of fermat’s factorization by considering the last m digits of modulus to decrease computation time., IJ Network Security 19 (1) (2017) 99–111.
- M. W. Bunder, J. Tonien, A new attack on the rsa cryptosystem based on continued fractions

对 RSA 变种的攻击:

- A. Takayasu, Y. Lu, L. Peng, Small crt-exponent rsa revisited, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2017, pp. 130–159
- M. Bunder, A. Nitaj, W. Susilo, J. Tonien, A new attack on three variants of the rsa cryptosystem, in: Australasian Conference on Information Security and Privacy, Springer, 2016, pp. 258–268.

总结：RSA 中的各个地方使用中都可能有坑，在不了解的情况下盲目实现可能在许多地方都会导致不安全

The End