RSA 密码系统

濯

2021 年 11 月 8 日

目录

1 RSA 背景

RSA 是 1977 年由罗纳德 · 李维斯特、阿迪 · 萨莫尔和伦纳德 · 阿德曼一起提出的。当时他们三人都在麻省理工学院工作。RSA 就是他们三人姓氏开头字母拼在一起组成的。

RSA 基于 $Euler$ 定理和大数的素因子分解非常困难。

2 加密原理

引理 2.1. *当 m 的素因数分解为 $p_1p_2\dots p_r$ 时*

$$a^{\varphi(m)+1} \equiv a\,(mod\, m)$$

证明: 只需证明 $p_i \mid a^{\varphi(m)+1} - a \qquad i = 1, 2, \dots, r$
注意到当 $p_i \mid a$ 时结论显然成立
只需证明 $(a, p_i) = 1$ 的情况, 即证 $a^{\varphi(m)} \equiv 1 \pmod{p_i}$
由费马小定理 $a^{p_i-1} \equiv 1 \pmod{p_i}$ 同时 $\varphi(m) = \prod_{i=1}^{r}(p_i - 1)$
因此 $a^{\varphi(m)} \equiv 1 \pmod{p_i}$ 进而 $a^{\varphi(m)+1} \equiv a \pmod{m}$ □

现在我们来具体说明 RSA 的实现原理。
设 $n = pq$,pq 是两个不同的大素数,α 是大于 p 和 q 的素数, 则存在 β 使得

$$\alpha\beta \equiv 1 \pmod{\varphi(n)}$$

这样对于任意整数 A,$0 \le A < n$, 必有唯一整数 B 满足

$$B \equiv A^{\alpha} \pmod{n} \quad 0 \le B < n$$

进而由引理得到

$$B^{\beta} \equiv A^{\alpha\beta} \equiv A \pmod{n} \quad 0 \le A < n$$

3 加密原理具体解释

现在小王公开声明了 n 和 α, 并且他已经知道了 n 的质因数分解, 小卓想给小王传递数据 A 但是害怕别人知道传递的是什么, 于是他将 A^{α} 对 n 取模后得到 B, 将 B 传给小王, 小王用 B 计算出 β 进而得到小卓真实想传递的数据 A。

由于其他人不知道 n 的质因数分解, 于是无法从小卓传递的信息中获取真实想要传递的数据 A。而正是 n 质因数分解的困难性保证了 RSA 的加密安全性。

4 加密实践

通过线性筛[1]小王得到了两个数量级在 10^7 的素数 pq 以及 α

其中 $n = pq = 2500085400729307, \alpha = 50000897$

现在假如你是小卓，你想向小王传递 2003211 这个数字，请问你该对小王输入什么?

[1] 又称作欧拉筛