AceBear 2019 - Baby RSA

Lê Quốc Dũng

April 2019

Đề bài rsa.py

Đặt $c1 = (p+q)^{2019}$, $c2 = (p+2019)^q$

$\Rightarrow (p+2019)^q - c2$ chia hết n

$\Rightarrow (p+2019)^q - c2$ chia hết q

$\Rightarrow (p+2019)^q \equiv c2$ mod q

Theo định lý Fermat, $(p+2019)^q \equiv p+2019$ mod q

$\Rightarrow p+2019 \equiv c2$ mod q

$\Rightarrow$ p+2019-c2 chia hết q

Mà ta cũng có n chia hết cho q

$\Rightarrow$ a*n + b*(c2-p-2019) chia hết q, với a, b là các số nguyên bất kì.

Ta có a*n + b*(c2-p-2019) = an + b(c2-2019) - b*p (1) nên ta sẽ tìm số a, b để a*n + b*(c2-2019) trở nên gọn nhất có thể. Bằng thuật toán Euclid ta tìm được gcd(n, c2-2019) = 1 nên ta dùng thuật toán Euclid mở rộng để tìm a, b để a*n + b*(c2-2019) = 1.

Thay a và b vào (1) ta có 1 - b*p chia hết q $\Rightarrow$ b*p - 1 = k*q $\Rightarrow$ b*p = k*q + 1 (2)

Ta lại có $(p+q)^{2019} \equiv c1$ mod n

$\Rightarrow (p+q)^{2019} \equiv c1$ mod q

$\Rightarrow (p+q)^{2019} * b^{2019} \equiv c1 * b^{2019}$ mod n

$\Rightarrow (b*p+b*q)^{2019} \equiv (c1*b^{2019})\%n$ mod n

Thay (2) vào đây $\Rightarrow (1+(k+b)*q)^{2019} \equiv (c1*b^{2019})\%n$ mod q.

Mà $1+(k+b)*q \equiv 1$ mod q $\Rightarrow (c1*b^{2019})\%n - 1$ chia hết q

$\Rightarrow gcd(n, (c1*b^{2019})\%n - 1) = q$ vì $(c1*b^{2019})\%n - 1$ không chia hết n.

$\Rightarrow$ Tìm ước chung lớn nhất giữa n và $(c1*b^{2019-1})\%n$ sẽ được q. Từ đó tính p và giải mã được bài toán.