__/__/__ S T Q Q S S D

4Q → Se b é invariante pelo RSA com chave (N, e) então $b^e \equiv b \pmod N$.
Portanto $b^e \equiv (\text{mod } p)$ e $b^e \equiv (\text{mod } q)$.

Resolvendo pelo Teorema Chinês do Resto, temos que:

$$\begin{cases} b^e \equiv b \pmod p \\ b^e \equiv b \pmod q \end{cases}$$

Onde:
$p = 3 \quad q > 3 \quad e = 3$

Pelo enunciado, sabemos que p e q são primos ímpares distintos.
Logo, $mdc(p, q) = 1$

Sendo $x = b^e$, temos que:

$$\begin{cases} x \equiv b \pmod p \\ x \equiv b \pmod q \end{cases}$$

Podemos converter as equações de congruências em identidades de inteiros.

Assim $x \equiv b \pmod p$ corresponde a $X = 1 + pk$, que é um inteiro e, como tal, pode ser substituído na segunda equação, o que dá:

$$b + pk \equiv b \pmod q$$

Substituindo $p = 3$ e q por um primo ímpar > 3 (Ex: 5), temos:

$$b + 3k \equiv b \pmod 5$$

Logo, $3k \equiv 0 \pmod 5$

spiral