# Alice

mensaje $x = 4$

$y = x^e \equiv 64 \mod 33$

$y = 31$

# Bob

1. Elegir $p = 3$ y $q = 11$
2. $n = p \cdot q = 33$
3. $\Phi(n) = (3-1)(11-1) = 20$
4. Elegir $e = 3$
5. $d \equiv e^{-1} \equiv 7 \mod 20$;
   *Donde* $d \cdot e = 7 \cdot 3 \equiv 1 \mod 20$

$k_pub = (33, 3)$ ←

$y = 31$ →

$y^d = 31^7 \equiv 4 = x \bmod 33$