IIC1253 Matemáticas Discretas

Sasha Kozachinskiy

DCC UC

26.11.2025

Hoy...

Teoría de números: pequeño teorema de Fermat, algoritmo RSA

Pequeño teorema de Fermat

Teorema

Si p es un número primo y $a \in \mathbb{Z}$ no es divisible por p, entonces $a^{p-1} \equiv_p 1$

Pequeño teorema de Fermat

Teorema

Si p es un número primo y $a \in \mathbb{Z}$ no es divisible por p, entonces $a^{p-1} \equiv_p 1$

Corolario

Si p es un número primo, entonces $a^p \equiv_p a$ para todo $a \in \mathbb{Z}$.

Ejercicio 1

Ejercicio

Encuentre $8^{900} \mathrm{mod} 29$

Ejercicio 2

Ejercicio

Encuentre $3^{2000} \mod 43$

Ejercicio 3

Ejercicio

Sea p un número primo. Demuestre que $p|7^p - 5^p - 2$.

Demostración de PTF: paso 0

“ a no es divisible por p” $\iff$ “a y p son coprimos”.

Demostración de PTF: paso 0

" a no es divisible por p" $\iff$ "a y p son coprimos".

Lema

Sean $x, y \in \mathbb{Z}$ dos números, no divisibles por p. Entonces, xy no es divisible por p.

Demostración de PTF: paso 1

Definición

Sea a un número entero, no divisible por p. Definimos $f_a\colon \{1,\ldots,p-1\} \to \{1,\ldots,p-1\}$, $f_a(x) = ax \bmod p$.

Demostración de PTF: paso 1

Definición

Sea a un número entero, no divisible por p. Definimos $f_a\colon \{1,\ldots,p-1\} \to \{1,\ldots,p-1\}$, $f_a(x) = ax \bmod p$.

Lema

Para todo número entero a, no divisible por p, la función f_a es biyectiva.

Demostración de PTF: paso 2

$$
\begin{aligned}
&1 \cdot 2 \cdot \ldots \cdot (p-1) \\
&= (a \cdot 1 \bmod p) \cdot (a \cdot 2 \bmod p) \cdot \ldots \cdot (a \cdot (p-1) \bmod p) \\
&\equiv_p (a \cdot 1)(a \cdot 2) \ldots (a \cdot (p-1)) \\
&= a^{p-1} 1 \cdot 2 \cdot \ldots \cdot (p-1).
\end{aligned}
$$

Demostración de PTF: paso 2

$$
\begin{aligned}
&1 \cdot 2 \cdot \ldots \cdot (p-1) \\
&= (a \cdot 1 \bmod p) \cdot (a \cdot 2 \bmod p) \cdot \ldots \cdot (a \cdot (p-1) \bmod p) \\
&\equiv_p (a \cdot 1)(a \cdot 2) \ldots (a \cdot (p-1)) \\
&= a^{p-1} 1 \cdot 2 \cdot \ldots \cdot (p-1).
\end{aligned}
$$

Por lo tanto

$$p | (a^{p-1} - 1) \cdot 1 \cdot 2 \cdot \ldots (p-1).$$

Demostración de PTF: paso 2

$$
\begin{aligned}
&1 \cdot 2 \cdot \ldots \cdot (p-1) \\
&= (a \cdot 1 \bmod p) \cdot (a \cdot 2 \bmod p) \cdot \ldots \cdot (a \cdot (p-1) \bmod p) \\
&\equiv_p (a \cdot 1)(a \cdot 2) \ldots (a \cdot (p-1)) \\
&= a^{p-1} 1 \cdot 2 \cdot \ldots \cdot (p-1).
\end{aligned}
$$

Por lo tanto

$$p | (a^{p-1} - 1) \cdot 1 \cdot 2 \cdot \ldots (p-1).$$

Ya que p es coprimo con $1, 2, \ldots, p-1$, obtenemos $p | (a^{p-1} - 1)$.

RSA

- ¿Enviar un mensaje al banco tal que nadie sea capaz entenderlo aparte del banco?
- El algoritmo RSA

RSA

- ¿Enviar un mensaje al banco tal que nadie sea capaz entenderlo aparte del banco?
- El algoritmo RSA

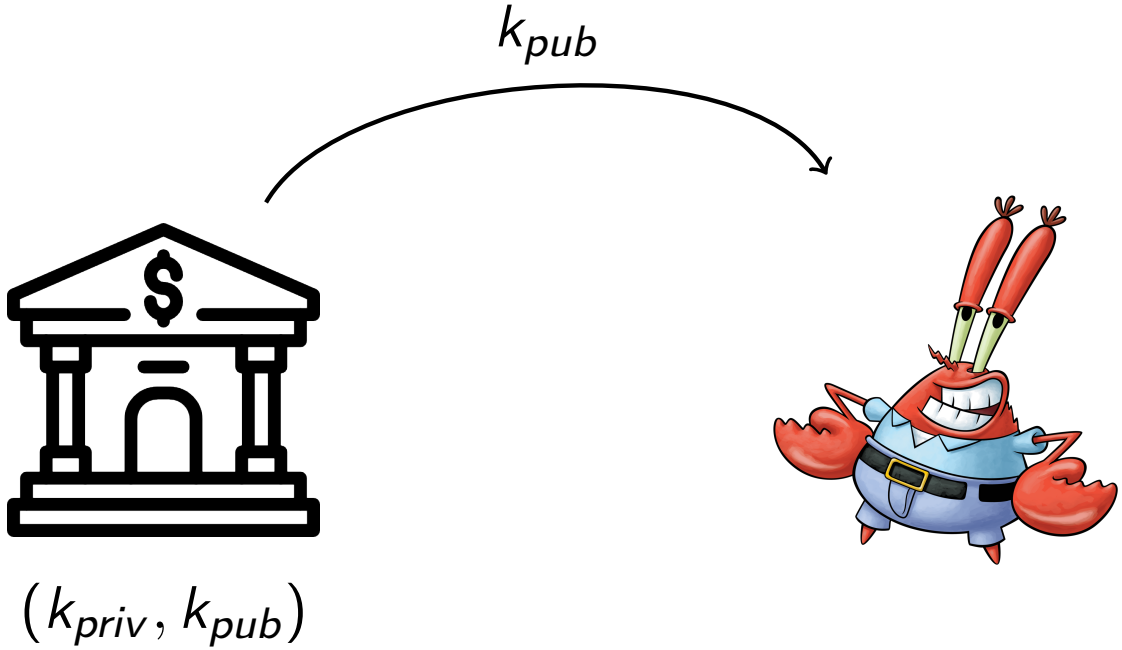
RSA

- ¿Enviar un mensaje al banco tal que nadie sea capaz entenderlo aparte del banco?
- El algoritmo RSA

(k_{priv}, k_{pub})

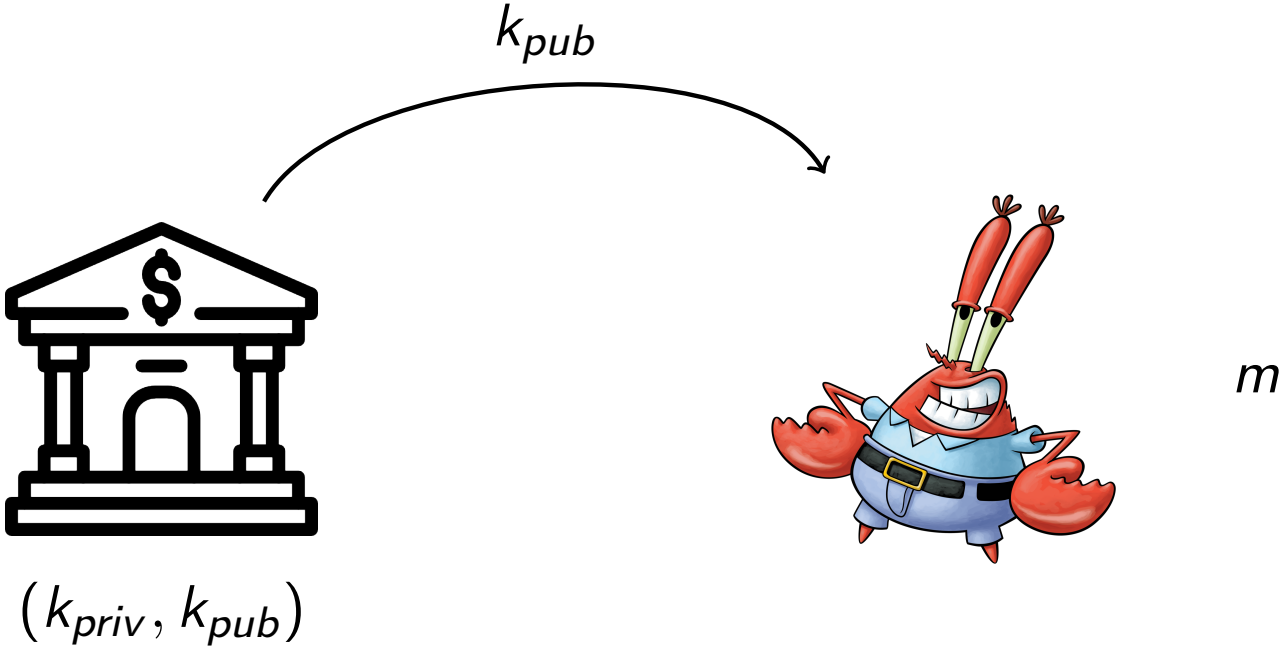
RSA

- ¿Enviar un mensaje al banco tal que nadie sea capaz entenderlo aparte del banco?
- El algoritmo RSA



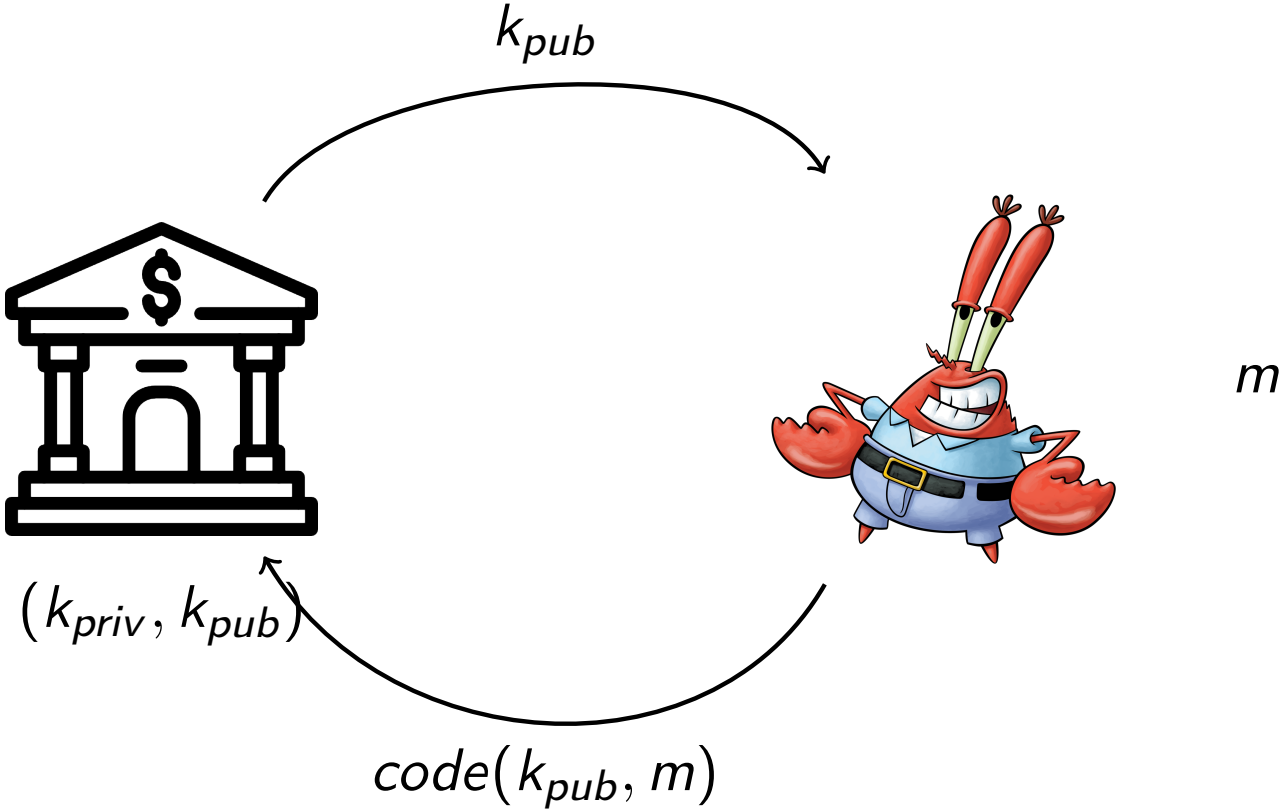
RSA

- ¿Enviar un mensaje al banco tal que nadie sea capaz entenderlo aparte del banco?
- El algoritmo RSA



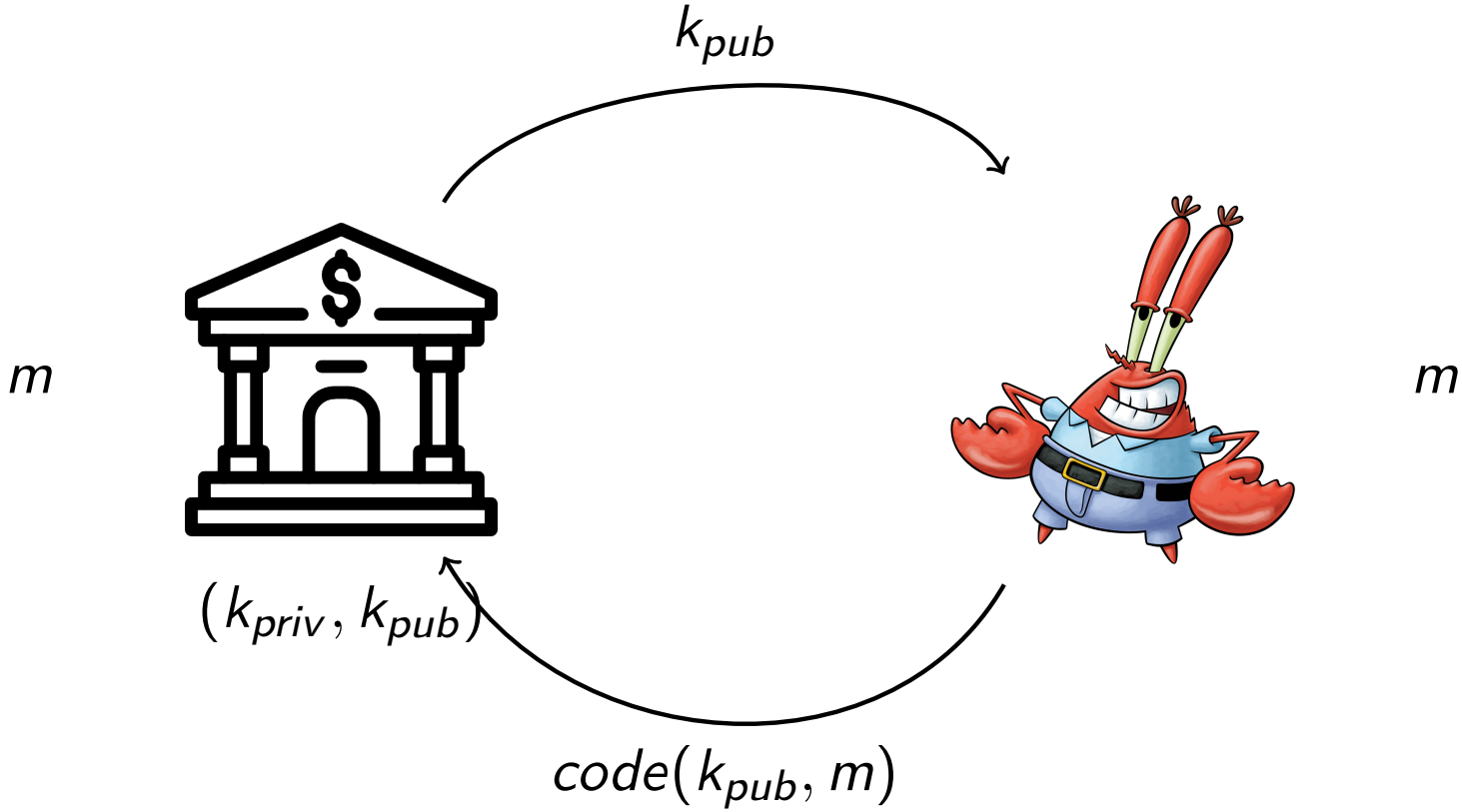
RSA

- ¿Enviar un mensaje al banco tal que nadie sea capaz entenderlo aparte del banco?
- El algoritmo RSA



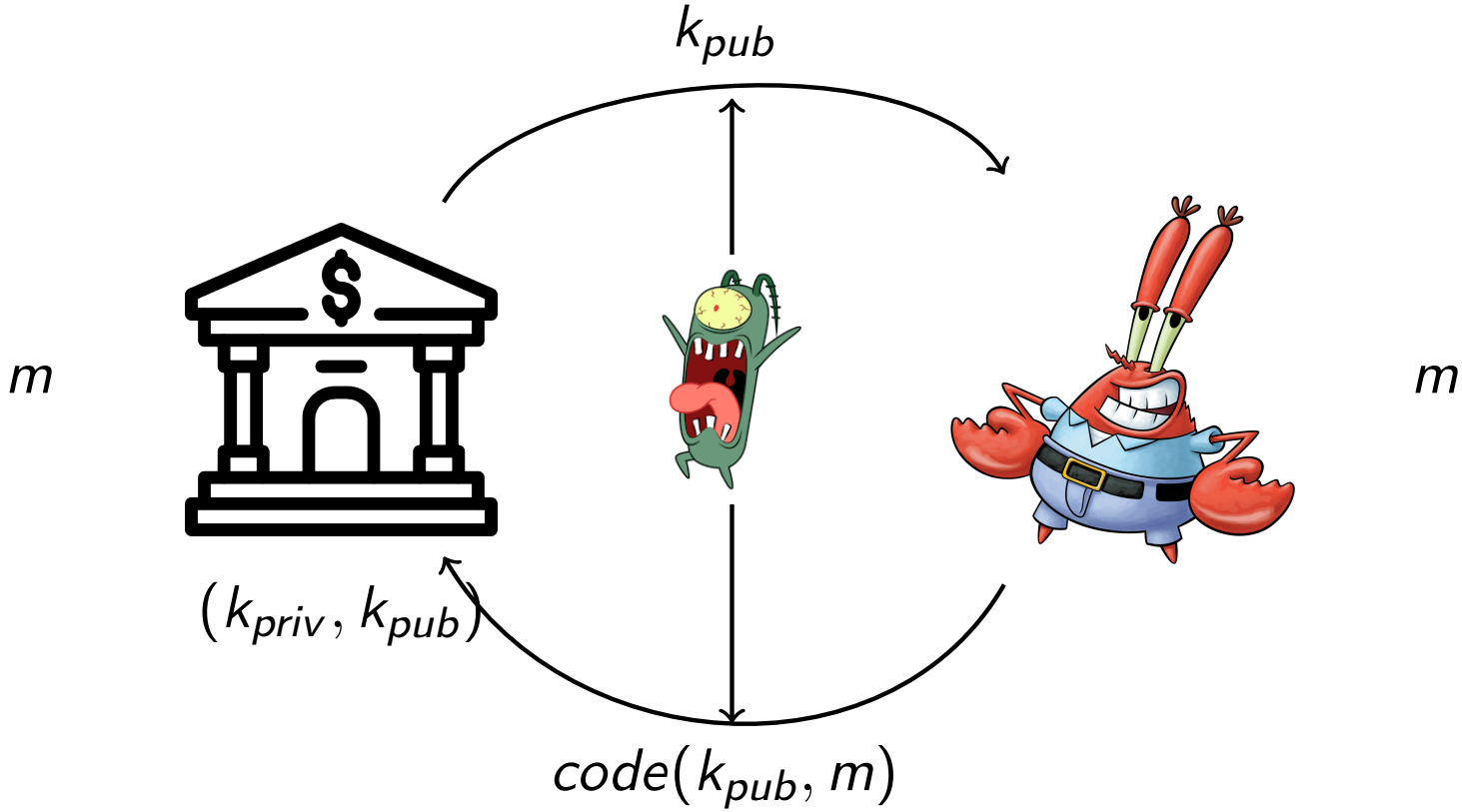
RSA

- ¿Enviar un mensaje al banco tal que nadie sea capaz entenderlo aparte del banco?
- El algoritmo RSA

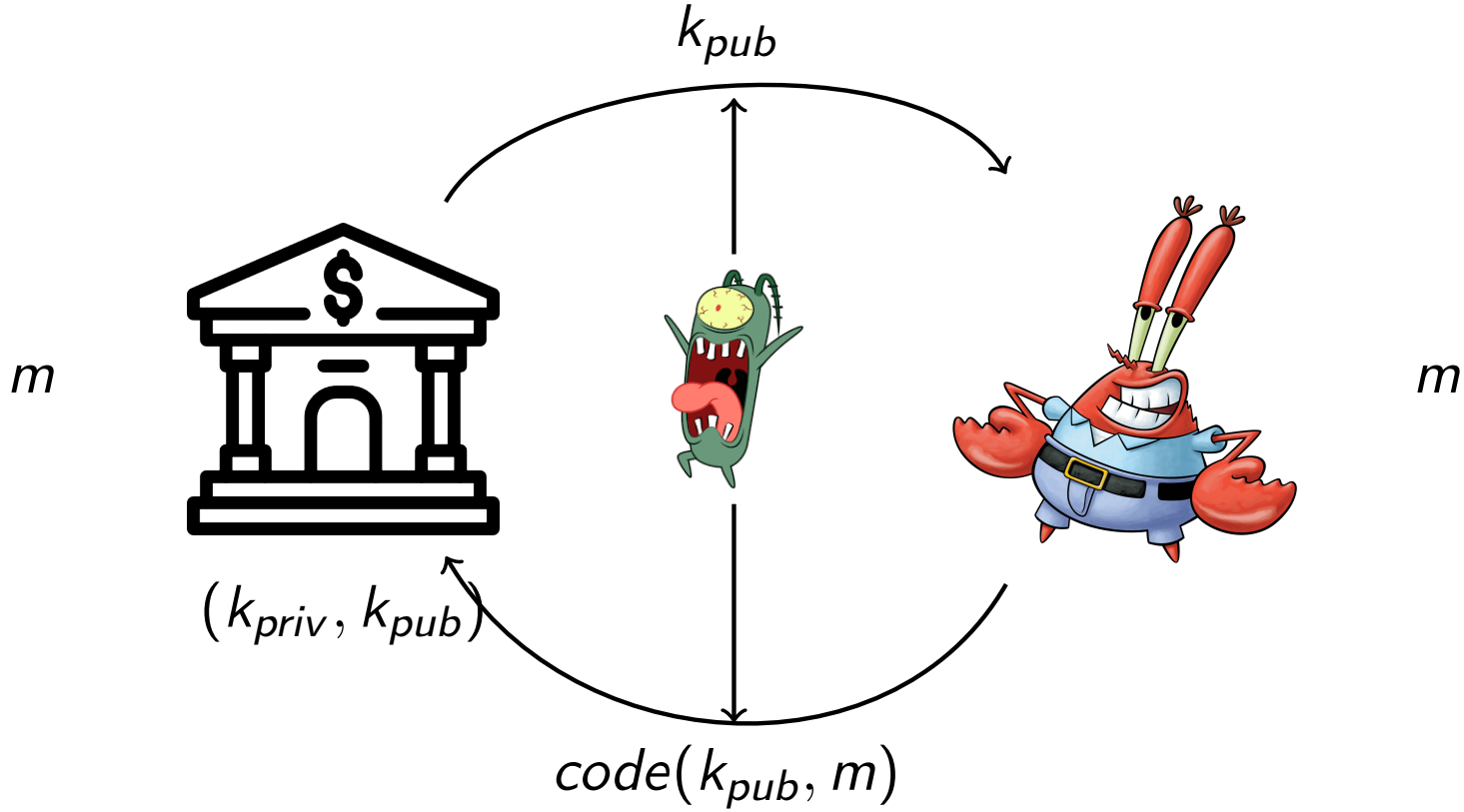


RSA

- ¿Enviar un mensaje al banco tal que nadie sea capaz entenderlo aparte del banco?
- El algoritmo RSA



El algoritmo



Lema

$m^{1+k(p-1)(q-1)} \equiv_{pq} m$ *para todo* $m, k \in \mathbb{Z}$.

Remarkas finales

- Fiabilidad del algoritmo $\Longrightarrow$ no existe un algoritmo rápido para descomposición en factores primos.

Remarkas finales

- Fiabilidad del algoritmo $\Longrightarrow$ no existe un algoritmo rápido para descomposición en factores primos.
- Shor (1999): existe un algoritmo *cuántico* rápido para descomposición en factores primos

Remarkas finales

- Fiabilidad del algoritmo $\Longrightarrow$ no existe un algoritmo rápido para descomposición en factores primos.
- Shor (1999): existe un algoritmo *cuántico* rápido para descomposición en factores primos
- computadores cuánticos...

Remarkas finales

- Fiabilidad del algoritmo $\Longrightarrow$ no existe un algoritmo rápido para descomposición en factores primos.
- Shor (1999): existe un algoritmo *cuántico* rápido para descomposición en factores primos
- computadores cuánticos...
- criptografía cuántica.

¡Gracias!