

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 $8^{900} \bmod 29$

Ejercicio 2

Ejercicio

Sean $a, b \in \mathbb{Z}$ tal que $p \neq 2, 5$ es un número primo y sea $a/p = \alpha_0, \alpha_1 \alpha_2 \alpha_3 \dots$. Demuestre que $\alpha_n = \alpha_{n+p-1}$ para todos $n \geq 1$.

Ejercicio 3

Ejercicio

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

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 $f_a: \{1, \dots, p-1\} \rightarrow \{1, \dots, p-1\}$, $f_a(x) = ax \bmod p$.

Demostración de PTF: paso 1

Definición

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

Lema

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

Demostración de PTF: paso 2

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

Demostración de PTF: paso 2

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

Por lo tanto

$$p \mid (a^{p-1} - 1) \cdot 1 \cdot 2 \cdot \dots \cdot (p-1).$$

Demostración de PTF: paso 2

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

Por lo tanto

$$p \mid (a^{p-1} - 1) \cdot 1 \cdot 2 \cdot \dots \cdot (p-1).$$

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

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

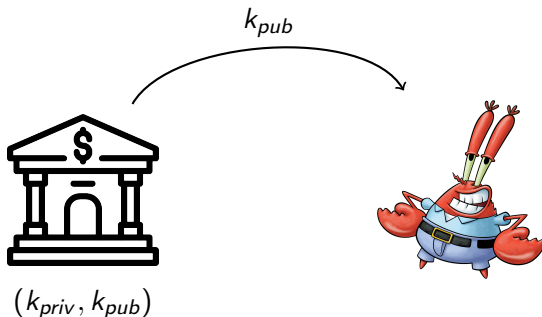
- ▶ ¿Enviar un mensaje al banco tal que nadie sea capaz entenderlo aparte del banco?
- ▶ El algoritmo RSA



(k_{priv}, k_{pub})

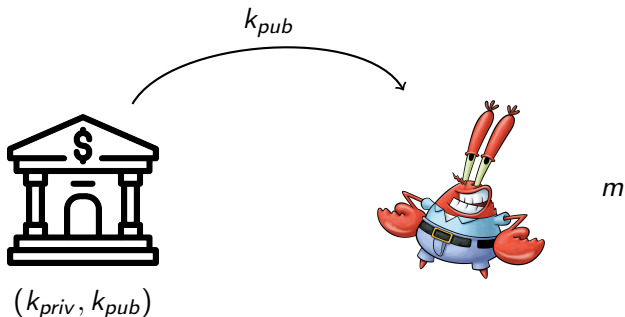
RSA

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



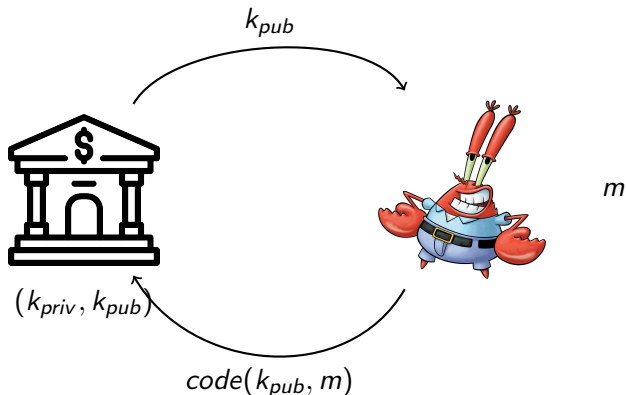
RSA

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



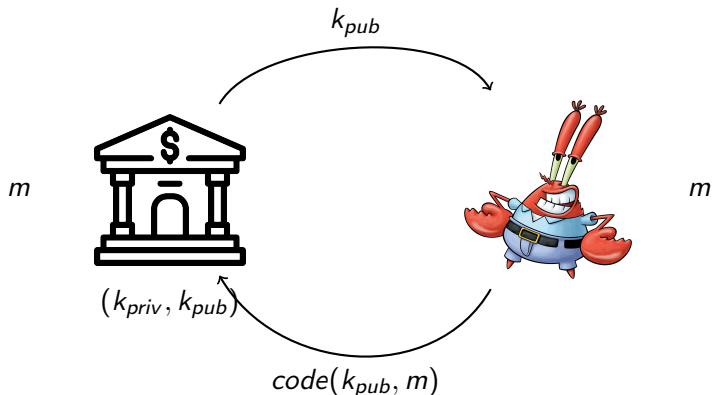
RSA

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



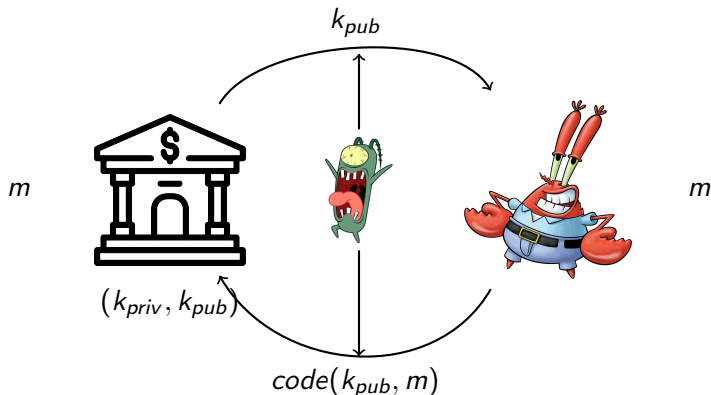
RSA

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

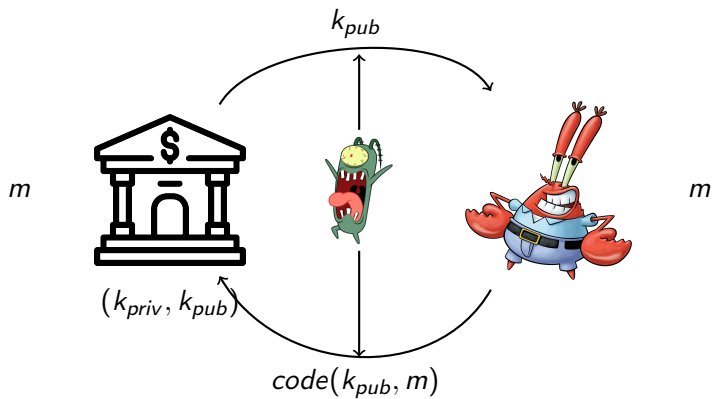


RSA

- ▶ ¿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 \implies no existe un algoritmo rápido para descomposición en factores primos.

Remarkas finales

- ▶ Fiabilidad del algoritmo \implies 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 \implies 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 \implies 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!