

# Una introducción a la teoría de números (y a la criptografía)

IIC1253

# Motivación: Criptografía de clave pública

Se tiene dos funciones  $E$  y  $D$ :

- ▶  $E$  sirve para encriptar y  $D$  para desencriptar:  $D(E(M)) = M$
- ▶  $E$  no puede usarse para desencriptar:  $E(E(M)) \neq M$
- ▶  $E$  y  $D$  están relacionadas, pero es difícil descubrir  $D$  a partir de  $E$

Vamos a ver un ejemplo de este tipo de sistemas: **RSA**

# El sistema criptográfico RSA

Algoritmo:

1. Adivine dos números primos distintos  $P$  y  $Q$
2. Sean  $N = P \cdot Q$  y  $\phi(N) = (P - 1) \cdot (Q - 1)$
3. Sean  $e$  y  $d$  dos números tales que  $(e \cdot d) \bmod \phi(N) = 1$
4. Entonces:

$$\begin{aligned} E(M) &= M^e \bmod N \\ D(M) &= M^d \bmod N \end{aligned}$$

Decimos que  $(e, N)$  es la clave pública y  $(d, N)$  es la clave privada

# El sistema criptográfico RSA

## Ejemplo

Sean  $P = 7$  y  $Q = 11$

- Se tiene que  $N = 77$  y  $\phi(N) = 60$

Sean  $e = 13$  y  $d = 37$

- Se tiene que  $(13 \cdot 37) \bmod 60 = 1$

Entonces:  $E(M) = M^{13} \bmod 77$  y  $D(M) = M^{37} \bmod 77$

Para  $M = 5$ :

$$\begin{aligned} E(5) &= 5^{13} \bmod 77 = 26 \\ D(E(5)) &= 26^{37} \bmod 77 = 5 \end{aligned}$$

# ¿Por qué funciona RSA?

¿Qué propiedades debemos demostrar que son ciertas?

- ▶  $D(E(M)) = M$  para todo  $M \in \{0, \dots, N - 1\}$

¿Qué problemas debemos demostrar que pueden ser resueltos de manera eficiente?

- ▶ Generar primos  $P$  y  $Q$ : Verificar si un número es primo
- ▶ Generar números  $e$  y  $d$  tales que  $(e \cdot d) \bmod \phi(N) = 1$
- ▶ Calcular funciones  $E$  y  $D$

¿Qué problemas no pueden ser resueltos de manera eficiente?

- ▶ Dado  $(e, N)$  calcular  $d$ : Encontrar los divisores de  $N$

Vamos a estudiar algunos conceptos de **Teoría de Números** necesarios para mostrar que RSA funciona y puede ser implementado.

# Componente fundamental de RSA: Aritmética modular

## Definición

$a \equiv b \pmod{n}$  si  $n$  divide a  $(b - a)$ .

Usamos la notación  $n|m$  para indicar que  $n$  divide a  $m$ .

►  $a \equiv b \pmod{n}$  si  $n|(b - a)$

Vamos a estudiar algunas propiedades fundamentales de  $\equiv$ .

# Aritmética modular: Propiedades básicas

## Proposición

$a \equiv b \pmod{n}$  si y sólo si  $a \pmod{n} = b \pmod{n}$ .

**Demostración:** ( $\Leftarrow$ ) Sabemos que:

$$\begin{array}{lll} a & = & \alpha \cdot n + \beta \quad 0 \leq \beta < n \\ b & = & \gamma \cdot n + \delta \quad 0 \leq \delta < n \end{array}$$

Por hipótesis:  $\beta = \delta$

► Puesto que  $a \pmod{n} = \beta$  y  $b \pmod{n} = \delta$

Tenemos que:  $(b - a) = (\gamma - \alpha) \cdot n$

► Por lo tanto:  $n \mid (b - a)$

# Aritmética modular: Propiedades básicas

( $\Rightarrow$ ) Suponga que  $a \bmod n \neq b \bmod n$

► Tenemos que  $\beta \neq \delta$  en las ecuaciones de la parte ( $\Leftarrow$ )

Sin pérdida de generalidad suponemos que  $\beta < \delta$

Se tiene que:

$$b - a = (\gamma - \alpha) \cdot n + (\delta - \beta)$$

Pero:  $1 \leq (\delta - \beta) \leq \delta < n$

► Por lo tanto:  $n \nmid (b - a)$





# Aritmética modular: Propiedades básicas

## Corolario

$$a \equiv (a \bmod n) \bmod n$$

## Ejercicio

Demuestre el corolario

# Aritmética modular: Propiedades básicas

## Proposición

Si  $a \equiv b \pmod{n}$  y  $c \equiv d \pmod{n}$ , entonces:

$$\begin{aligned}(a + c) &\equiv (b + d) \pmod{n} \\ (a \cdot c) &\equiv (b \cdot d) \pmod{n}\end{aligned}$$

## Ejercicios

1. Demuestre la proposición
2. Demuestre que un número  $n$  es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3
3. De reglas de división para los números 4 y 8

# Aritmética modular: Una propiedad fundamental

## Teorema (Fermat)

*Sea  $p$  un número primo. Si  $a \in \{0, \dots, p-1\}$ , entonces  $a^p \equiv a \pmod{p}$ .*

**Demostración:** Por inducción en  $a$

Para  $a = 0$  y  $a = 1$  se cumple trivialmente. Suponga que  $a^p \equiv a \pmod{p}$  y  $2 \leq (a+1) < p$

Sabemos que:

$$(a+1)^p = \sum_{k=0}^p \binom{p}{k} a^k$$

# Aritmética modular: Una propiedad fundamental

Por lo tanto:

$$(a + 1)^p - (a + 1) = (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^k$$

## Lema

Si  $k \in \{1, \dots, p-1\}$ , entonces  $p \mid \binom{p}{k}$

**Demostración:** Sabemos que:

$$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!} = \frac{p \cdot (p-1) \cdot \dots \cdot (p-k+1)}{k!}$$

Como  $k \in \{1, \dots, p-1\}$  y  $p$  es un número primo:

$\frac{(p-1) \cdot \dots \cdot (p-k+1)}{k!}$  es un número entero

# Aritmética modular: Una propiedad fundamental

Por lo tanto:  $\binom{p}{k} = p \cdot \alpha$ , donde  $\alpha$  es un número entero

► Concluimos que  $p \mid \binom{p}{k}$



Del lema concluimos que  $p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^k$

Por lo tanto, dado que  $p \mid (a^p - a)$  por hipótesis de inducción, tenemos que:  $p \mid ((a+1)^p - (a+1))$

► Concluimos que  $(a+1)^p \equiv (a+1) \pmod{p}$



# Aritmética modular: Una propiedad fundamental

## Corolario (Fermat)

*Sea  $p$  un número primo. Si  $a \in \{1, \dots, p-1\}$ , entonces  $a^{p-1} \equiv 1 \pmod{p}$ .*

**Demostración:** Por teorema anterior sabemos que

$$a^p \equiv a \pmod{p}$$

Por lo tanto: existe un número entero  $\alpha$  tal que

$$a^p - a = \alpha \cdot p$$

# Aritmética modular: Una propiedad fundamental

Dado que  $a|(a^p - a)$ , se tiene que  $a|(\alpha \cdot p)$

Por lo tanto, dado que  $a \in \{1, \dots, p-1\}$  y  $p$  es un número primo, se concluye que  $a|\alpha$

Entonces:  $(a^{p-1} - 1) = \frac{\alpha}{a} \cdot p$ , donde  $\frac{\alpha}{a}$  es un número entero.

► Concluimos que  $a^{p-1} \equiv 1 \pmod{p}$



# RSA funciona correctamente

Sean  $E$  y  $D$  construidas como fue mencionado en las transparencias anteriores.

►  $N = P \cdot Q$ ,  $E(M) = M^e \bmod N$  y  $D(M) = M^d \bmod N$

## Teorema (Rivest-Shamir-Adleman)

*Para cada  $M \in \{0, \dots, N - 1\}$ , se tiene que  $D(E(M)) = M$ .*

**Demostración:** Sabemos que

$$\begin{aligned} D(E(M)) &= (M^e \bmod N)^d \bmod N \\ &= (M^e)^d \bmod N \\ &= M^{e \cdot d} \bmod N \end{aligned}$$

Por lo tanto, tenemos que demostrar que  $M^{e \cdot d} \equiv M \bmod N$



# RSA funciona correctamente: Demostración

Sabemos que  $e \cdot d \equiv 1 \pmod{\phi(N)}$

► Por lo tanto:  $e \cdot d = k \cdot \phi(N) + 1$

Tenemos que demostrar que  $M^{k \cdot \phi(N) + 1} \equiv M \pmod{N}$

► El siguiente lema es fundamental para la demostración

## Lema

$$M^{k \cdot \phi(N) + 1} \equiv M \pmod{P} \text{ y } M^{k \cdot \phi(N) + 1} \equiv M \pmod{Q}$$

**Demostración:** Primero suponemos que  $P|M$ .

# RSA funciona correctamente: Demostración

$$\begin{aligned}\text{Entonces: } M^{k \cdot \phi(N) + 1} \bmod P &= (M \bmod P)^{k \cdot \phi(N) + 1} \bmod P \\ &= 0^{k \cdot \phi(N) + 1} \bmod P \\ &= 0\end{aligned}$$

Por lo tanto:  $M^{k \cdot \phi(N) + 1} \equiv M \bmod P$

En segundo lugar, suponemos que  $P \nmid M$ .

► Sea  $R = M \bmod P$

Dado que  $R \in \{1, \dots, P - 1\}$ , por teorema de Fermat:

$$R^{P-1} \equiv 1 \bmod P$$

Por lo tanto, dado que  $R \equiv M \bmod P$ :

$$M^{P-1} \equiv 1 \bmod P$$

# RSA funciona correctamente: Demostración

De esto concluimos que:

$$\begin{aligned} M^{k \cdot \phi(N) + 1} \bmod N &= ((M^{P-1})^{k \cdot (Q-1)} \cdot M) \bmod P \\ &= ((M^{P-1} \bmod P)^{k \cdot (Q-1)} \cdot M) \bmod P \\ &= (1^{k \cdot (Q-1)} \cdot M) \bmod P \\ &= M \bmod P \end{aligned}$$

Concluimos que  $M^{k \cdot \phi(N) + 1} \equiv M \bmod P$

- De la misma forma se demuestra que  $M^{k \cdot \phi(N) + 1} \equiv M \bmod Q$



# RSA funciona correctamente: Demostración

Del lema concluimos que:

$$M^{k \cdot \phi(N) + 1} - M = \alpha \cdot P$$

$$M^{k \cdot \phi(N) + 1} - M = \beta \cdot Q$$

Por lo tanto:  $\alpha \cdot P = \beta \cdot Q$

Entonces, dado que  $P$  y  $Q$  son primos distintos tenemos que  $P | \beta$

$$\blacktriangleright \beta = \gamma \cdot P$$

Concluimos que  $M^{k \cdot \phi(N) + 1} - M = \gamma \cdot P \cdot Q$

► Vale decir:  $M^{k \cdot \phi(N) + 1} \equiv M \pmod{N}$

