RSA

A

$n = pq$,

sabe p, q

Sabe calcular

$\varphi(n) = (p-1)(q-1)$

Sabe que

e coprimo con $\varphi(n)$

$\Rightarrow$ puede calcular

$d = e^{-1} \mod \varphi(n)$

$de \equiv 1 \pmod{\varphi(n)}$

Datos Públicos

(n, e)

Clave pública

de Alice

$y = x^e \mod n$

B

Sabe x

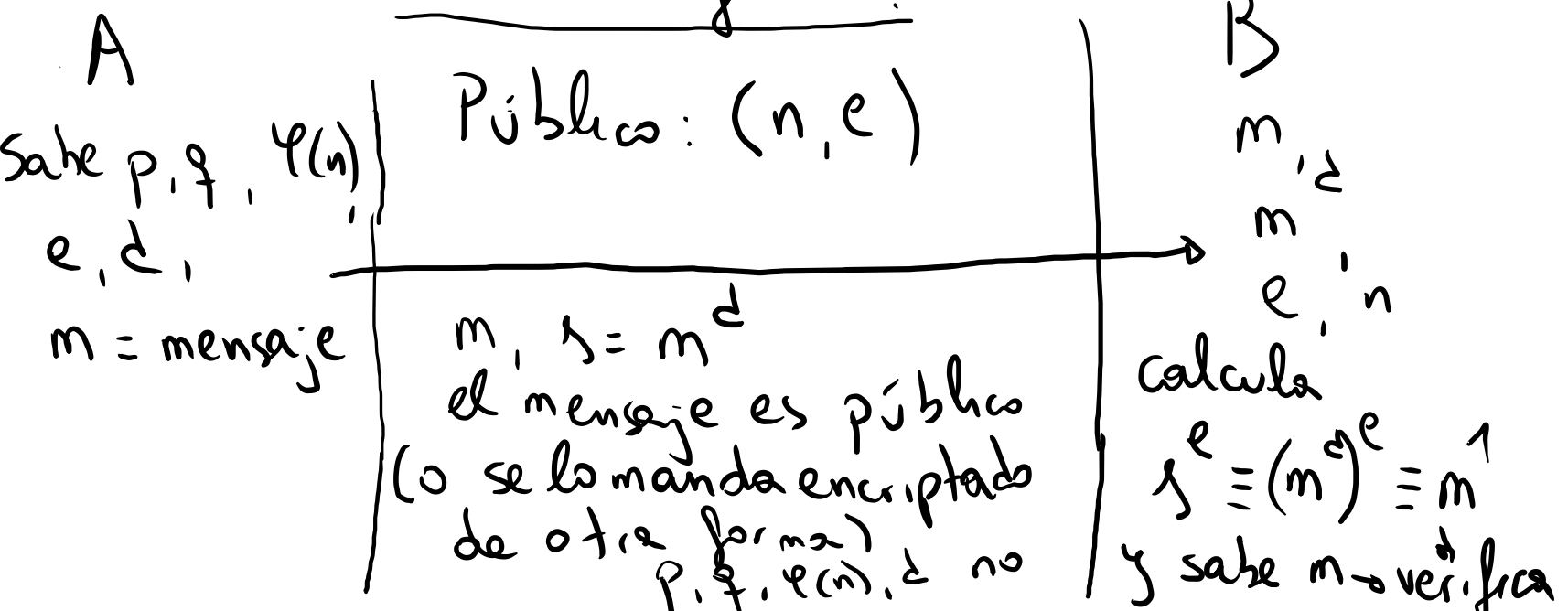
(lo que quiere mandar)

Alice calcula $y^d \pmod n$

$$y^d \equiv (x^e)^d \equiv x^{ed} \equiv x^1 \pmod n$$

↓ desencriptó x.

Firma digital



8) Alice manda 3 documentos a Bob

x, y, z . firmados

Clave de Alice = $(10379, 17)$ (lo sabe Bob)

Sea $d = 17^{-1} \mod \varphi(10379)$

Bob recibe

$x, s = x^d$, $y, t = y^d$, $z, u = z^d$

sabe que $s^{17} = x$, $t^{17} = y$, $u^{17} = z$

} con esto intenta averiguar d (anda a saber cómo)

Bob falsifica la firma de Alice.

manda (m, f)

↳ firma falsa.

Lo que tendría que pasar es que $f^{17} \equiv m \pmod{10379}$

Si Bob falsificó sin éxito, no le da la igualdad

(hacer la cuenta para los 4 casos)

ECB (n, e) clave pública

Texto de Letras ⟶ número módn

Texto de Letras ⟵ número encriptado módn

encriptadas si queremos

MATERIA

¿qué tamaño de bloque máximo puedo encriptar?

Letras ⟷ números de 0 a 27 (En ASCII de 0 a 128, 256)

Con k cifras puedo obtener 28^k números.

necesito que $28^k < n < 28^{k+1}$

Si $n = 606409$

$28^2 = 784$, $28^3 = 21.952$, $28^4 = 614.656$

$k = 3$

MATERIA

diccionario

MAT

12 0 20

$12\,28^2 + 0 \cdot 28^1 + 20 \cdot 28^0$

da un nº entre 0 y $606409 - 1 < 28^4 - 1$ → este nº

Texto → lo escribo en base 28 con 4 cifras. → lo llevo a la 1111 encriptado.