NÚMEROS B-LISOS

EJEMPLO: SEA $N = 636683$. QUEREMOS HALLAR UN FACTOR (NO TRIVIAL) DE N.

SI HALLAMOS $a, b \in \mathbb{Z}$ / $a^2 \equiv b^2 \ (N)$, ENTONCES

$a^2 - b^2 = (a-b)(a+b) = k \cdot N$.

$\rightsquigarrow$ CALCULANDO $\gcd(a \pm b, N)$ QUIZÁS LO OBTENGAMOS.

PARA ELLO TENEMOS LO SIGUIENTE:

- $1387^2 \equiv 13720 \ (N)$, Y $13720 = 2^3 \cdot 5 \cdot 7^3$
- $2774^2 \equiv 54880 \ (N)$, Y $54880 = 2^5 \cdot 5 \cdot 7^3$

$\rightsquigarrow$ ASÍ, $(\underbrace{1387 \cdot 2774}_{=:a})^2 \equiv (\underbrace{2^4 \cdot 5 \cdot 7^3}_{=:b})^2 \ (N)$

PERO: $\gcd(a-b, N) = N$, $\gcd(a+b, N) = 1$, POR LO QUE ESTOS VALORES DE a Y b NO SIRVEN.

TENEMOS, ADEMÁS:

- $3359^2 \equiv 459270 \ (N)$, Y $459270 = 2 \cdot 3^8 \cdot 5 \cdot 7$

$\rightsquigarrow (\underbrace{1387 \cdot 3359}_{=:a})^2 \equiv (\underbrace{2^2 \cdot 3^4 \cdot 5 \cdot 7^2}_{=:b})^2 \ (N)$,

Y SE TIENE $\gcd(a-b, N) = 797$. ESTO NOS DA $N = 797 \cdot 809$

RECORDAR: SEA $B > 0$. $m \in \mathbb{N}$ ES B-LISO SI

$$p \mid m \Rightarrow p \leq B.$$ (OBS: UN TAL m DEBERÍA SER FÁCIL DE FACTORIZAR SI B ES CHICO)

EJ: 13720, 54880, 459270 SON 7-LISOS.

LO IMPORTANTE: SI $B = L(N)^{1/\sqrt{2}}$, CON $L(X) = e^{\sqrt{\ln(x)\ln(\ln(x))}}$,

- BASTA CON CONSIDERAR NÚMEROS a_i / $a_i^2 \pmod N$ SEA B-LISO PARA FACTORIZAR N. (CRECE LENTAMENTE!)
- LA CANTIDAD DE B-LISOS QUE HACE FALTA PARA FACTORIZAR N ES APROX. $L(N)^{\sqrt{2}}$: //

¿CÓMO DECIDIR SI m ES B-LISO?

ALGORITMO

1. FOR $p \leq B$ PRIMO: [illegible]
2. WHILE $p \mid m$: [illegible]
3. $m = m/p$
4. IF $m = 1$:
5. RETURN TRUE
6. ELSE:
   RETURN FALSE //

LOS NÚMEROS B-LISOS SE PUEDEN USAR PARA CALCULAR $\log$ EN $\mathbb{Z}/p^\times$. [illegible]

EJEMPLO: SEAN $p = 18443$, $g = 37$. g ES RAÍZ PRIMITIVA EN $\mathbb{Z}/p^\times$. QUEREMOS CALCULAR $\log_g(211) \in \mathbb{Z}/p-1$.

IDEA: SI $211 \cdot g^{-k}$ ES B-LISO, ENTONCES $\log_g(211) \equiv k +$ "$\log g$'s DE PRIMOS $p \leq B$" $\pmod{p-1}$. 1/2

1. BUSCAMOS POTENCIAS DE g QUE SEAN 5-LISAS.

POR EJ,

$$g^{12708} \equiv 2^3 \cdot 3^4 \cdot 5 \quad (p)$$
$$g^{15400} \equiv 2^3 \cdot 3^3 \cdot 5 \quad (p)$$
$$g^{11311} \equiv 2^3 \cdot 5^2 \quad (p)$$

↘ AL MENOS TRES...

2. ASÍ, SI LLAMAMOS $x_q = \log_g(q)$ $(q = 2,3,5)$ TENEMOS QUE

$$\begin{cases} 12708 \equiv 3x_2 + 4x_3 + x_5 \quad (p-1) \\ 15400 \equiv 3x_2 + 3x_3 + x_5 \quad (p-1) \\ 11311 \equiv 3x_2 + 2x_5 \quad (p-1) \end{cases}$$

↝ SIST. DEL QUE QUEREMOS DESPEJAR x_2, x_3, x_5. PERO $p-1$ NO ES PRIMO!

SIENDO $p-1 = 2 \cdot \underbrace{9221}_{\text{PRIMO}}$,

EL SIST. ES EQUIVALENTE A

$$\begin{cases} 0 \equiv x_2 + x_3 \quad (2) \\ 0 \equiv x_2 + x_3 + x_5 \quad (2) \\ 1 \equiv x_2 \quad (2) \end{cases}$$

↝ SOL $(1,0,1)$ (mód 2)

$$\begin{cases} 3497 \equiv 3x_2 + 4x_3 + x_5 \quad (9221) \\ 6179 \equiv 3x_2 + 3x_3 + x_5 \quad (9221) \\ 2090 \equiv 3x_2 + 2x_5 \quad (9221) \end{cases}$$

↝ SOL $(5733, 6529, 6277)$ (mód 9221).

VÍA TEO CHINO, TENEMOS QUE LA SOL ES

$$(5733, 15750, 6277) \quad (\text{mód } p-1)$$

3. $211 \cdot g^{-9549}$ (mód p) ES 5-LISO,

↑ BUSCO UN EXPONENTE k TAL QUE $211 \cdot g^{-k}$ LO SEA...

/3

DE HECHO

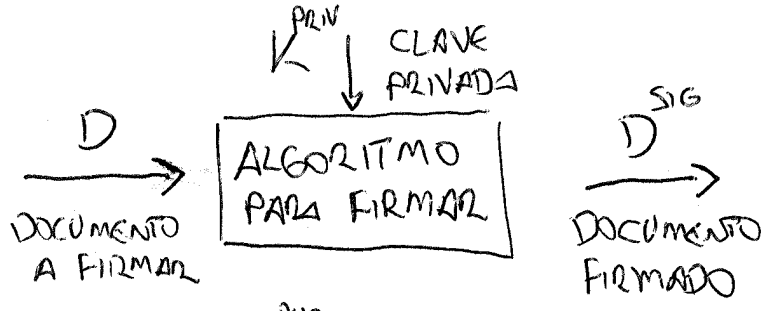
$$211 \cdot g^{-9549} \equiv 2^5 \cdot 3^2 \cdot 5^2 \pmod{p}$$

4. $$\log_g(211) \equiv 9549 + 5 \cdot x_2 + 2 \cdot x_3 + 2 \cdot x_5$$
$$\equiv 8500 \pmod{p-1}.$$

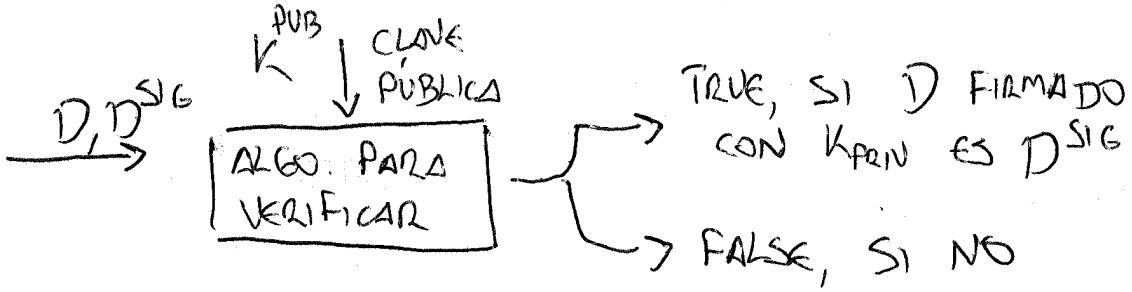
FIRMAS DIGITALES Y RSA

ESQUEMÁTICAMENTE, UNA FIRMA DIGITAL ES LO SIGUIENTE

1.



2.



EJEMPLO: TOMO PRIMOS p, q, $N = p \cdot q$, ELIJO

V / [illegible] $(V : N) = 1$, Y CALCULO

[illegible] S / $S \cdot V \equiv 1 \pmod{(p-1)(q-1)}$.

- $K^{PRIV} = S$, $K^{PUB} = V$
- ALGO PARA FIRMAR: $D \longmapsto D^S$
- ALGO PARA VERIFICAR: [illegible] $S^V == D$

OBS: PARA EVITAR USAR FIRMAS DEL TAMAÑO DEL MENSAJE, SE FIRMA EN LUGAR DE D A $h(D)$ CON h FUNCIÓN HASH