CLASE PRÁCTICA 23/5

ASÍ, ENCRIPTAR ES RÁPIDO

1. RSA MULTIPRIMO

EN LA VERSIÓN "TRADICIONAL" DE RSA, SE TOMA $N = p \cdot q$ CON p, q PRIMOS, $3 \leq e < N$ EXPONENTE "CHICO" Y $1 \leq d < N$ / $d \cdot e \equiv 1 \ ((p-1)(q-1))$

PROBLEMA: d PUEDE SER DEL ORDEN DE N, CASO EN EL QUE DESENCRIPTAR ES LENTO.

EN LUGAR DE DOS PRIMOS, TOMAMOS $p_1, \dots, p_k$ PRIMOS $(k \geq 2)$, $N = p_1 \cdot \dots \cdot p_k$.

e: $3 \leq e < N$, $(e : \varphi(N)) = 1$

$\varphi(N) = \prod (p_i - 1)$

d: $1 \leq d < N$ / $d \cdot e \equiv 1 \ (\varphi(N))$.

SIGUE VALIENDO QUE $(m^e)^d \equiv m \ (N)$.

OBS: NO HACE FALTA USAR d, SI USAMOS EL TEO CHINO DEL RESTO.

- SEA $1 \leq d_i < p_i - 1$ / $d_i \cdot e \equiv 1 \ (p_i - 1)$
- SEA $m_i \equiv c^{d_i} \ (p_i)$

VENTAJA: LOS d_i SON MÁS CHICOS QUE d

• SEA m' LA SOLUCIÓN A

$$\begin{cases} X \equiv m_1 \ (p_1) \\ \vdots \\ X \equiv m_u \ (p_u) \end{cases}$$

AFIRMO: $m' = m$ (ES DECIR, OBTENEMOS EL MENSAJE)

DEM: BASTA VER QUE $m' \equiv m \ (p_i) \quad \forall i$;

EN EFECTO,

$$m' \equiv m_i \equiv C^{d_i} \equiv m^{e \cdot d_i} \equiv m \ (p_i), \text{ PUES}$$

$e \cdot d_i \equiv 1 \ (p_i)$ ✓ ☒

OBS: EL TEO CHINO TAMBIÉN SE PUEDE USAR SI $u = 2$.

2. MILLER-RABIN

INPUT: ENTEROS m y a, $1 \leq a < m$.

OUTPUT: → m ES COMPUESTO
→ EL TEST FALLA (a NO ES UN TESTIGO DE MILLER-RABIN PARA LA "COMPOSITENESS" DE m)

TEO: SI m ES COMPUESTO,

$$\frac{\#\{1 \leq a < m : a \text{ ES TESTIGO}\}}{m-1} \geq 3/4$$

DADO m, SUPONGAMOS QUE EL TEST FALLA PARA k VALORES DE a ELEGIDOS AL AZAR. LA PROBABILIDAD DE QUE m SEA COMPUESTO* ES $< (1/4)^k$.

$\rightsquigarrow$ LA "PROB DE QUE m SEA PRIMO" ES $> 1-(1/4)^k$.

QUIERO: "ASEGURARME" DE QUE UN NÚMERO m ES PRIMO.

HAGO:
- ELIJO UN $0 < \lambda < 1$ (CERCANO A 1).
- TOMO $k \in \mathbb{N}$ / $1-(1/4)^k \geq \lambda$ ES DECIR, $1-\lambda \geq (1/4)^k$, O SEA $\frac{\log_2(1-\lambda)}{2} \leq k$.
- EJECUTO MILLER-RABIN PARA k VALORES DE a ELEGIDOS AL AZAR ENTRE 1 Y $m-1$
- SI EL TEST DICE QUE m ES COMPUESTO PARA ALGÚN a, LISTO
- SI EL TEST FALLA LAS k VECES Y m ES COMPUESTO, NOS ENCONTRAMOS ANTE UN EVENTO DE PROBABILIDAD $0 < 1-\lambda < 1$ (CERCANO A 0)

*MEJOR DICHO: LA PROB. DE QUE, SIENDO m COMPUESTO, SUCEDA ESTO...

3. GENERAR PRIMOS GRANDES

QUEREMOS: p PRIMO DE TAMAÑO m EN BITS (POR EJ, $m = 128$)

LUEGO: • ELIJO UN NÚMERO m AL AZAR DE m BITS

• EJECUTO M-R k VECES SOBRE m.

↳ ¿CÓMO LO HAGO?

1° PONGO $m = 0$

2° PARA $0 \leq i \leq m-1$:

3° ELIJO UN "BIT" AL AZAR $b \in \{0,1\}$.

4° SI $b = 1$, PONGO $m = m + 2^i$

5° RETURN m.

↝ ASÍ, $m = \sum_{i=0}^{m-1} b_i \cdot 2^i$

LUEGO, EL PROBLEMA SE REDUCE A TENER UN GENERADOR DE BITS ALEATORIOS...