PRÁCTICO 1

1. EL ALGORITMO "ELEVAR AL □ Y MULTIPLICAR"

PROBLEMA: DADOS $g, A, N \in \mathbb{N}$, CALCULAR $g^A \bmod N$;
NOS INTERESA PORQUE SON CUENTAS QUE HAREMOS PARA ENCRIPTAR INFORMACIÓN.

SOLUCIÓN (MALA): MULTIPLICAR $g \cdot g \cdot \dots \cdot g$ A VECES
$\rightsquigarrow$ SON A MULTIPLICACIONES.

SOLUCIÓN (BUENA): • ESCRIBIR $A = A_0 \cdot 2^0 + \dots + A_{r-1} 2^{r-1} + A_r 2^r$
CON $A_i \in \{0,1\}$, $A_r = 1$ "DESARROLLO EN BASE 2"

VALE $r = O(\log_2 A)$ ($A \geq 2^r$)

• CALCULAR

$$a_0 \equiv g \ (N)$$
$$a_1 \equiv a_0^2 \equiv g^2 \ (N)$$
$$a_2 \equiv a_1^2 \equiv (g^2)^2 \ (N)$$
$$\vdots$$
$$a_r \equiv (a_{r-1})^2 \equiv g^{2^r}$$

} r MULTIPLICACIONES

• $g^A \equiv g^{\sum A_i 2^i} = \prod_{i \text{ con } A_i \neq 0} g^{2^i}$ $\rightsquigarrow \leq r$ MULTIPLICACIONES

$\rightsquigarrow$ EN TOTAL $\leq 2r$ MULTIPLICACIONES ✓
$\leq 2 \log_2 A$

2. $\mathbb{F}_p^*$

RECORDAR: $\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ $\rightsquigarrow$ GRUPO CÍCLICO DE ORDEN $p-1$

LUEGO, EXISTE $g \in \mathbb{F}_p^*$ TAL QUE $\mathbb{F}_p^* = \{1, g, \dots, g^{p-2}\}$

¿CUÁNTAS RAÍCES PRIMITIVAS HAY?

$a = g^e$ ES PRIMITIVA SII $(e : p-1) = 1$

$\rightsquigarrow$ HAY $\varphi(p-1)$ RAÍCES PRIMITIVAS.

EJEMPLO: $p = 31$, BUSCAMOS UNA RAÍZ PRIMITIVA, ie, DE ORDEN $30 = 2 \cdot 3 \cdot 5$ $\rightsquigarrow$ BUSCO RAÍCES DE ÓRDENES 2, 3, 5.

- $2^5 \equiv 32 \equiv 1 \ (31)$ $\rightsquigarrow$ $\mathrm{ord}(2) = 5$.
- $\{\text{RAÍCES DE ORDEN } 2\} = \{\text{RAÍCES DE } X^2 - 1\} \setminus \{1\}$

  $\rightsquigarrow$ $-1 \equiv 30$ TIENE ORDEN 2.
- DE ORDEN 3: SEA $a \in \mathbb{F}_{31}^*$. SI $a^{\frac{30}{3}} = a^{10} \neq 1 \ (31)$ ENTONCES a^{10} TIENE ORDEN 3! PUES $(a^{10})^3 \equiv 1 \ (31)$.

  $\rightsquigarrow$ PRUEBO.

  $3^{10} \equiv 3^{2+2^3} \equiv 3^2 \cdot 3^{2^3} \equiv 9 \cdot 20 \equiv 180 \equiv 25$

  CA: $3^2 = 9 \ (31)$; $3^{2^2} \equiv 81 \equiv 19 \ (31)$; $3^{2^3} \equiv 19^2 \equiv 361 \equiv 20 \ (31)$

$\rightsquigarrow$ SOL: $2 \cdot 30 \cdot 25 \equiv -50 \equiv 12 \ (31)$ ES PRIMITIVA

EJERCICIO: HALLAR UNA RAÍZ PRIMITIVA EN $\mathbb{F}_{2311}^*$.

3. UN EJEMPLO DE ENCRIPTADO

TOMAMOS p UN PRIMO. PARA $k \in \mathbb{F}_p^*$, CONSIDERAMOS $e_k : \mathbb{F}_p \to \mathbb{F}_p$, $m \mapsto (k^2+1)\cdot m$. ¿ES UNA FUNCIÓN DE ENCRIPTADO? PARA ESO, DEBERÍA EXISTIR $d_k : \mathbb{F}_p \to \mathbb{F}_p$ TAL QUE $d_k(e_k(m)) = m$.

IDEA: $d_k(C) = \frac{1}{k^2+1} \cdot C$ ⇝ PERO PODRÍA SER $k^2+1 = 0$! (EN CUYO CASO NO EXISTE e_k)

SOLUCIÓN: TOMAR p TAL QUE $-1 \neq \square\,(p)$, ie $p \equiv 3\ (4)$.

UNA BUENA FUNCIÓN DE ENCRIPTADO DEBE TENER LAS SIG. CUATRO PROPIEDADES:

I) e_k FÁCIL DE CALCULAR ✓

II) d_k " " " ✓

III) DADOS $C_1, \dots, C_m$ MENSAJES CIFRADOS ¿PUEDO HALLAR $d_k(C_1), \dots, d_k(C_m)$ SIN CONOCER k?

NO... PERO SÍ SI CONSIGO $e_k : \mathbb{Z} \to \mathbb{Z}$! (CÁLCULO MCD)

IV) NO VULNERABLE A UN ATAQUE DE TEXTO PLANO:

NO LA TIENE. SI CONOZCO PARA ALGÚN m EL VALOR $C = e_k(m)$, ENTONCES DESPEJO $k^2+1 = C/m$, Y DE ACÁ OBTENGO $\pm k$...

MEJOR: PLANTEAR $e_k : \mathbb{Z} \to \mathbb{Z}$, NOTAR QUE II FALLA, PERO QUE COMPLICA USAR $e_k : \mathbb{F}_p \to \mathbb{F}_p$.