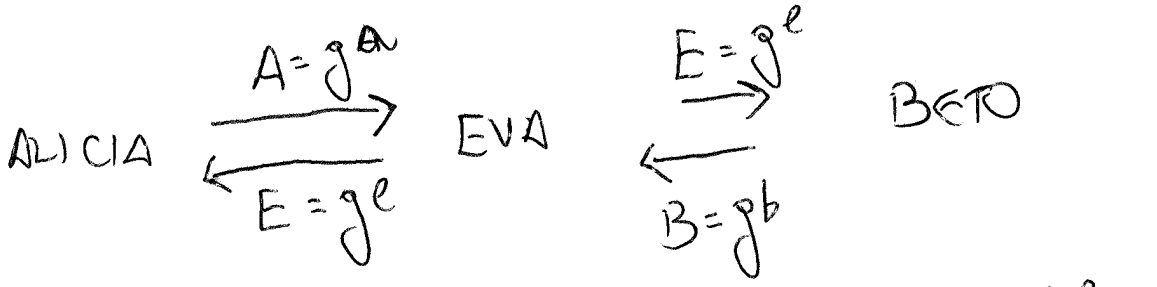
PRÁCTICO 3

1. EL ATAQUE HOMBRE-EN-EL-MEDIO

DIFFIE-HELLMAN: p PRIMO, $g \in \mathbb{F}_p^*$

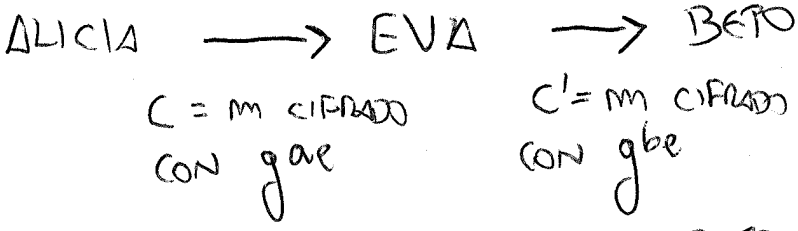
- ENTEROS SECRETOS, ALICIA a BETO b
- ALICIA LE ENVÍA A BETO $g^a = A$
  BETO " " " ALICIA $g^b = B$
- ALICIA CALCULA $A^b = g^{ab}$
  BETO " $B^a = g^{ab}$
  } CLAVE PRIVADA COMPARTIDA (A SER USADA COMO CLAVE DE UN CIFRADO SIMÉTRICO)

SI EVA LOGRA "PONERSE EN EL MEDIO":



⇝ ALICIA Y EVA COMPARTEN LA CLAVE g^{ae}
BETO " " " " " g^{be}

SI ALICIA QUIERE ENVIAR A BETO UN MENSAJE m:



⇝ EVA PUEDE CALCULAR m; BETO OBTIENE m SIN SABER QUE EVA ESTÁ EN EL MEDIO!

NOTAR: EVA LOGRÓ DESENCRIPTAR m SIN PREOCUPARSE EN ABSOLUTO POR EL PROBLEMA DEL LOGARITMO DISCRETO!

2. ROMPER RSA VS FACTORIZAR N

VIMOS QUE SI EVA LOGRA FACTORIZAR $N = pq$, ENTONCES PUEDE HALLAR EL EXPONENTE DE DESENCRIPTADO RESOLVIENDO

$$de \overset{\text{DATO}}{\equiv} 1 \quad (\varphi(N)).$$

RECÍPROCAMENTE, SUPONGAMOS QUE EVA DE ALGUNA MANERA ENCONTRÓ d TAL QUE

$$a^{de} \equiv a \quad (N) \qquad (\forall\ a \ \because\ \varphi(N) \mid de-1)$$

$\forall\ a$ COPRIMO CON N. ¿CÓMO PUEDE UTILIZAR d PARA FACTORIZAR N?

IDEA: $x^2 \equiv 1\ (N)$ TIENE CUATRO SOLUCIONES:

± 1 Y $\pm x_0$, CON x_0 TAL QUE

$$\begin{cases} x_0 \equiv 1\ (p) \\ x_0 \equiv -1\ (q) \end{cases} \qquad \boxed{\exists!\ \text{: T.C.R.}}$$

- SON SOL ✓
- SON TODAS: SI $x^2 \equiv 1\ (N)$, $\begin{cases} x^2 \equiv 1\ (p) \\ x^2 \equiv 1\ (q) \end{cases}$ ✓

LUEGO

ENTONCES, SI $x^2 \equiv 1\ (N)$ Y $x \not\equiv \pm 1\ (N)$, ENTONCES

$$\gcd(\underbrace{x-1}_{\text{SUP. } x \neq 2;\ \text{SI } x=2,\ \text{USAR } x+1}, N) = \begin{cases} p, & \text{SI } x = x_0 \\ q, & \text{SI } x = -x_0 \end{cases}$$

$\rightsquigarrow$ LOGRAMOS FACTORIZAR N.

• CÓMO HALLAR UN TAL x? EL MÉTODO DE MILLER-RABIN DA RAÍCES □ DE 1. MÁS PRECISAMENTE,

FACTORIZO $de-1 = 2^s \cdot m$, CON $s, m \in \mathbb{N}$.
↳ ES POSITIVO PUES $(p-1)(q-1)$ ES PAR

TOMO $y \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}$ AL AZAR.

- SI $(y:N) \neq 1$, TENGO UN FACTOR DE N.
- SI NO:
  - SI $y^m \equiv 1$: ELIJO OTRO y
  - SI NO: TOMO $r_0 = \min\{r : y^{m \cdot 2^r} \equiv 1\}$ (≥ 1)
  - TOMO $x = y^{m \cdot 2^{r_0 - 1}}$; CUMPLE $x^2 \equiv 1$
    - SI $x \not\equiv \pm 1$: TENGO LO QUE BUSCABA
    - SI NO, ELIJO OTRO y

PROP: LA PROB. DE QUE y SIRVA ES $\geq 1/2$

SE DICE QUE ESTE ES UN ALG. PROBABILÍSTICO DE TIPO LAS VEGAS

DEM (IDEA): CONTAR LOS $y \in (\mathbb{Z}/N\mathbb{Z})^\times$ TALES QUE

- $y^m \equiv 1$ ó
- $\exists\, 0 \leq t < s$ / $y^{m \cdot 2^t} \equiv -1$

"LOS y QUE NO SIRVEN",

Y VER QUE SON MENOS DE LA MITAD ⊠

3. EL TEO. DE LOS NÚMEROS PRIMOS

SEA $\pi(x) = \#\{p \in \mathbb{N} : p \leq x,\ p \text{ PRIMO}\}$.

TEO: $\pi(x) / (x/\ln(x)) \longrightarrow 1$ $\quad x \to +\infty$

¿CÓMO PODEMOS USARLO PARA "CALCULAR" PRIMOS GRANDES?

PROP: DADO $N \in \mathbb{N}$, SEA

$P(N)$ = PROB. DE QUE UN $m \in (N/2, 3/2 N]$ (NATURAL) SEA PRIMO.

ENTONCES,

$$\frac{P(N)}{1/\ln(N)} \xrightarrow[N\to\infty]{} 1.$$

DEM:

$$P(N) = \frac{\#\{m \in (N/2, 3/2N] : m \text{ ES PRIMO}\}}{\#\{m \in (N/2, 3N/2]\}}$$

$$= \frac{\pi(3/2N) - \pi(N/2)}{\left[\frac{3N}{2}\right] - \left[\frac{N}{2}\right]} = \frac{\pi(3/2N) - \pi(N/2)}{N+\delta}, \text{ CON } |\delta| < 2.$$

$\downarrow$ $[\alpha] = \alpha + \varepsilon$, CON $|\varepsilon| < 1$

ENTONCES,

$$\frac{P(N)}{1/\ln(N)} = \frac{\ln(N)\,\pi(3N/2)}{N(1+\delta/N)} - \frac{\ln(N)\,\pi(N/2)}{N(1+\delta/N)}$$

$$= \frac{(\ln(3/2N) - \ln(3/2))\,\pi(\frac{3N}{2})}{3/2\,N(1+\delta/N)} \cdot \frac{3}{2} - \frac{(\ln(1/2N) - \ln(1/2))\,\pi(N/2)}{1/2\,N(1+\delta/N)} \cdot 1/2$$

$\xrightarrow[N\to\infty]{} 3/2 - 1/2 = 1$ ☒ (Y N ES GRANDE)

ASÍ, SI ELIJO k NÚMEROS AL AZAR EN $(N/2, 3/2N]$, LA PROB. DE QUE NINGUNO SEA PRIMO ES $\approx$

$$\left(1 - 1/\ln(N)\right)^k$$

EJ: SI N TIENE 1024 BITS, Y QUIERO UN PRIMO EN $(N/2, 3N/2]$ CON $\geq 90\%$ DE PROBABILIDAD, BASTA CON TOMAR 1634 NÚMEROS AL AZAR.