LOGARITMO DISCRETO

DADOS n, a, x CON $\text{mcd}(n, a) = 1$ ES

COMPUTACIONALMENTE FÁCIL CALCULAR: $a^x \bmod n$

PERO, DADOS n, a CON $\text{mcd}(n, a) = 1$ Y $1 < y < n$, ES

COMPUTACIONALMENTE DIFÍCIL:

ENCONTRAR x TAL QUE $a^x \equiv y \bmod n$

$x = \log_a y$

$\log_{10} 100 = 2$

$10^2 = 100$

CALCULAR EXPONENCIACIÓN: FÁCIL

CALCULAR LOGARITMO: DIFÍCIL (EN GENERAL) ← A VECES ES FÁCIL

USAREMOS $n = p$ PRIMO, ASÍ $\text{mcd}(p, a) = 1$

¿a? → g GENERADOR GRUPO MULTIPLICATIVO $(\mathbb{Z}/p\mathbb{Z})^*$

$\left(\mathbb{Z}/p\mathbb{Z}\right)^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ GRUPO MULTIPLICATIVO

SABEMOS QUE $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ ES UN GRUPO MULTIPLICATIVO DE ORDEN $p-1$

↑ GRUPO: PODEMOS OPERAR SUS ELEMENTOS SIN SALIRNOS

↑ MULTIPLICA-: OPERACIÓN

↑ ORDEN: NÚMERO DE ELEMENTOS

SEA g UN GENERADOR DE $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$, ES DECIR

$$\mathbb{Z}_p \setminus \{0\} = \mathbb{Z}/p\mathbb{Z} \setminus \{0\} = \{g^0, g^1, \ldots, g^{p-2}\} \quad (g^{p-1} = 1)$$

$g^0 = 1$

ORDEN DE g: $\text{ord}(g) = p-1$ $\quad (\min\{e \mid g^e = 1\})$

¿MEJOR FORMA DE ENCONTRAR g? PROBANDO DIFERENCIA GENERAL)

DES ELEMENTOS

PARA CUALQUIER ENTERO $A \in \{1, 2, \ldots, P-1\}$

EXISTE UN EXPONENTE $x \in \{0, 1, \ldots, P-2\}$ TAL QUE

$$A = g^x \bmod P$$

x: LOGARITMO DISCRETO DE A EN LA BASE g

$$x = \log_g A$$

Ej: $P = 13 \quad g = 2$

$\log_2 3 = 4 \quad 2^4 = 3 \bmod 13$

A	1	2	3	4	5	6	7	8	9	10	11	12
$\log_2 A$	0	1	4	2	9	5	11	3	8	10	7	6

$\log_2 7 = 11 \quad 2^{11} = 7 \bmod 13$

$2 = g^1$ $\quad 4 = g^2$ $\quad 8 = g^3$ $\quad \boxed{16 = 3 = g^4}$ .....

$\log_2 3 = 4$ PORQUE $2^4 = 3$

UNA TABLA ES LA ÚNICA ALTERNATIVA

g GENERADOR MULTIPLICATIVO DE $\mathbb{Z}_p \setminus \{0\}$

O RAÍZ PRIMITIVA MÓDULO p

$$\langle g \rangle = \{ g^0, g^1, \dots, g^{p-2} \} = \mathbb{Z}_p \setminus \{0\}$$

LA ELECCIÓN DE g NO ES ÚNICA, HAY VARIOS ELEMENTOS QUE CUMPLEN ESTA FUNCIÓN.

PERO: LA DIFICULTAD DE RESOLVER EL PROBLEMA DE LOGARITMO DISCRETO ES INDEPENDIENTE DEL GENERADOR QUE HAYAMOS ELEGIDO.

DEM:

SUPONGAMOS QUE ES FÁCIL CALCULAR LOGARITMOS DISCRETOS EN BASE g

SEA g' OTRO GENERADOR

¿ES FÁCIL O DIFÍCIL CALCULAR UN LOGARITMO DISCRETO CON LA BASE g'?

BUSCAMOS $x = \log_{g'} A$, DADO $A \in \mathbb{Z}_p^*$ $(g'^x = A \bmod p)$

PERO...

DADO $A \in \mathbb{Z}_p^*$ PODEMOS CALCULAR FÁCILMENTE

$w = \log_g g'$ $\quad (g^w \equiv g' \bmod p)$

$z = \log_g A$ $\quad (g^z \equiv A \bmod p)$

NOSOTROS BUSCAMOS $x = \log_{g'} A$

$A = g'^x \equiv (g^w)^x = g^{wx}$ Y $A \equiv g^z \bmod p$

$\Rightarrow g^{wx} = g^z \bmod p$

$\Rightarrow wx = z \mod p-1$ ← OJO

$\Rightarrow x = w^{-1} z \mod p-1$

(CONOCEMOS w Y z)

UN DETALLE: NOS FALTA PROBAR QUE w TIENE INVERSO MÓDULO $p-1$, ES DECIR: $\mathrm{mcd}(w, p-1) = 1$

SEA d / $d \mid w$ Y $d \mid p-1$ (UN DIVISOR COMÚN)

$$g^{\frac{p-1}{d}} \overset{\circledast}{=} \left(g^{w}\right)^{\frac{p-1}{d}} = \left(g^{p-1}\right)^{\frac{w}{d}} \overset{\uparrow \text{ord } g = p-1}{=} 1^{w/d} = 1$$

$$\Rightarrow \text{ord}(g') \leq \frac{p-1}{d} \overset{\uparrow \text{ord } g' = p-1}{\Rightarrow} d = 1 \Rightarrow \mathrm{mcd}(w, p-1) = 1$$

□

ELECCIÓN DE g

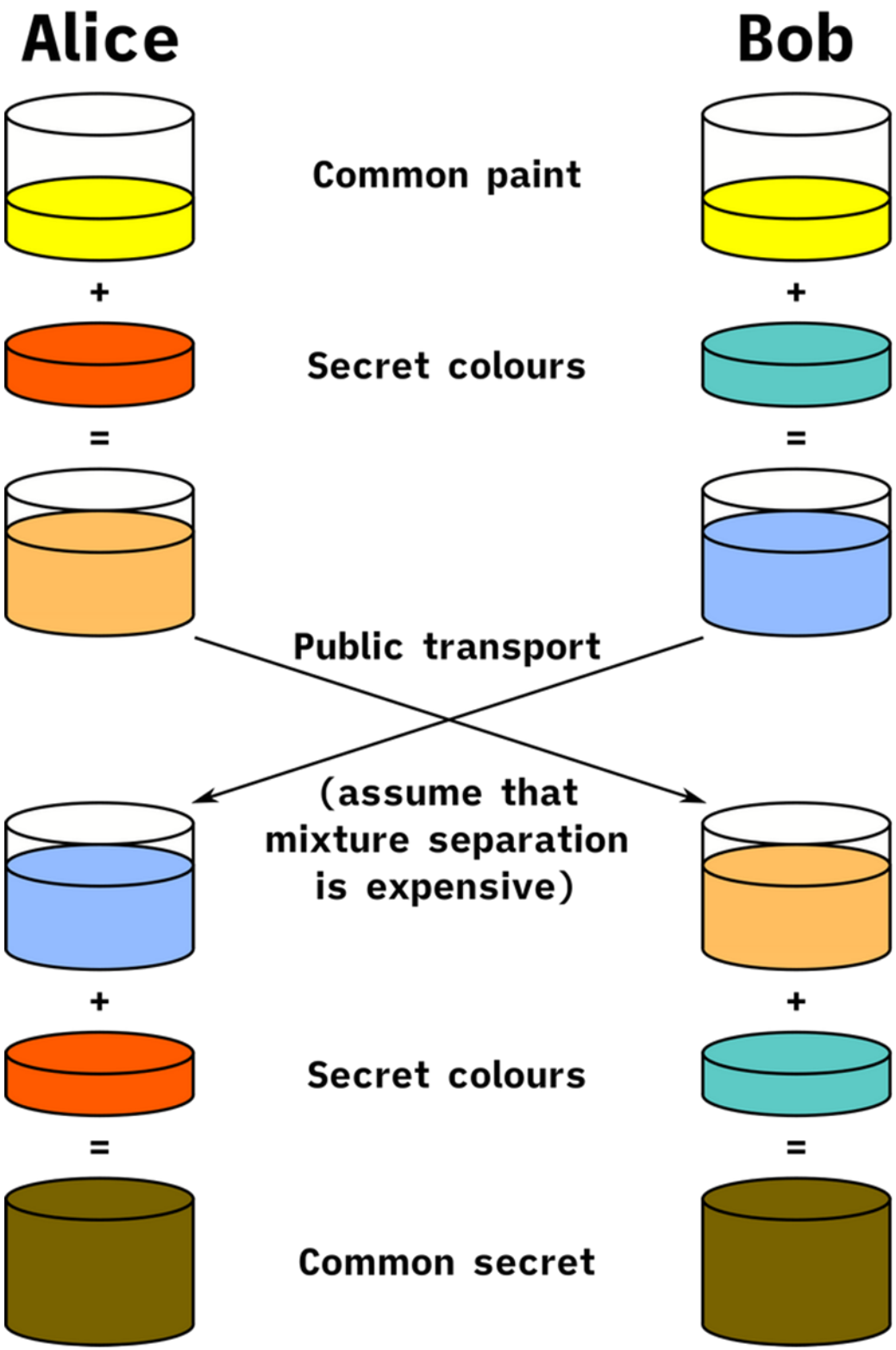
IDEALMENTE g SE TOMA DE ORDEN $p-1$, ES DECIR UN GENERADOR DEL GRUPO MULTIPLICATIVO $(\mathbb{Z}_p)^*$. PERO DADO SU TAMAÑO, ESTE PROBLEMA PUEDE SER DIFÍCIL Y UNO SE CONFORMA CON UN ELEMENTO CON UN ORDEN SUFICIENTEMENTE GRANDE.

$$\{g^0, g^1, g^2, g^3, \dots, g^N\} \quad \text{y} \quad g^{N+1} = 1$$

$\neq 1 \quad \neq 1 \quad \neq 1 \quad \neq 1$

$N < p-1$ PERO N GRANDE $\Rightarrow$ NOS VALE

AUNQUE $\{g^0, \dots, g^N\} \subsetneq \mathbb{Z}_p^*$



EXPLICACIÓN INTERCAMBIO CLAVES DIFFIE-HELLMAN CON COLORES

(FUENTE WIKIPEDIA)

INTERCAMBIO DE CLAVES DE DIFFIE-HELLMAN

ALICE Y BOB QUIEREN PONERSE DE ACUERDO EN UNA CLAVE PERO SÓLO PUEDEN COMUNICARSE A TRAVÉS DE UN CANAL INSEGURO

- PRIMERO, SE PONEN DE ACUERDO EN UN PRIMO p GRANDE Y EN UN ENTERO g, $2 \leq g \leq p-2$, TAL QUE EL ORDEN DE g MODULO p ES SUFICIENTEMENTE GRANDE.

TANTO p Y g SE PUEDEN CONSIDERAR PÚBLICOS

- ALICE ESCOGE UN ENTERO $a \in \{2, \ldots, p-2\}$ DE FORMA ALEATORIA, CALCULA

$$A = g^a \bmod p$$

Y SE LO ENVÍA A BOB

ALICE GUARDA a EN SECRETO

- BOB ESCOGE UN ENTERO $b \in \{2, \ldots, p-2\}$ DE FORMA ALEATORIA, CALCULA

$$B = g^b \bmod p$$

Y SE LO ENVÍA A ALICE

BOB GUARDA b EN SECRETO

- PARA OBTENER LA CLAVE SECRETA

  - ALICE CALCULA:

$$B^a \bmod p = (g^b)^a = g^{ab} \bmod p$$

  - BOB CALCULA:

$$A^b \bmod p = (g^a)^b = g^{ab} \bmod p$$

- LA CLAVE COMÚN ES $K = g^{ab} \bmod p$

EJ: $p = 17$, $g = 3$

ALICE: $a = 7 \Rightarrow A = g^a \bmod p = 3^7 \bmod 17 = 11$

ALICE $\xrightarrow{A = 11}$ BOB

BOB: $b = 4 \Rightarrow B = g^b \bmod p = 3^4 \bmod 17 = 13$

ALICE $\xleftarrow{B = 13}$ BOB

VER SAGE

ALICE: $B^a \bmod p = 13^7 \bmod 17 = 4 = K$

BOB: $A^b \bmod p = 11^4 \bmod 17 = 4 = K$

CLAVE COMÚN SECRETA

SEGURIDAD DIFFIE-HELLMAN

LA CRIPTOANALISTA EVE CONOCE P, g, A Y B.

PERO NO CONOCE $a = \log_g A$ Y $b = \log_g B$

¿COMO PODRÍA CALCULAR $K = g^{ab} \bmod P$?

PODRÍA CALCULAR $\log_g A$ (= a) Y $\log_g B$ (= b)

Y ENTONCES TENDRIA $K = g^{ab} \bmod P$.

SIN EMBARGO CALCULAR UN LOGARITMO DISCRETO ES COMPUTACIONALMENTE INTENSO

- TAMPOCO ES FACTIBLE EL ATAQUE DE DECISIÓN:

DADOS $g^a \bmod p$, $g^b \bmod p$ Y $g^c \bmod p$,

DECIDIR SI $g^{ab} = g^c$

- ATAQUE "MAN IN THE MIDDLE"

EVE INTERCEPTA LOS MENSAJES ENTRE ALICE Y BOB

E INTERCAMBIA UNA CLAVE CON ALICE Y BOB

SE PUEDE PREVENIR USANDO FIRMAS DIGITALES

LOS LOGARITMOS DISCRETOS SE PUEDEN CONSIDERAR EN GRUPOS ABELIANOS FINITOS ARBITRARIOS

GRUPO ABELIANO: UN CONJUNTO G CON UNA OPERACIÓN INTERNA "$\cdot$" QUE SATISFACE:

- PROPIEDAD ASOCIATIVA: $a\cdot(b\cdot c)=(a\,b)\cdot c$
- PROPIEDAD CONMUTATIVA: $a\cdot b = b\cdot a$
- ELEMENTO NEUTRO: $\exists\ e=1\in G\ /\ e\cdot a=a\cdot e=a,\ \forall a\in G$
- ELEMENTO INVERSO: $\forall a\in G,\ \exists\ a^{-1}\in G\ /\ a\cdot a^{-1}=a^{-1}\cdot a=1$

PERO HAY GRUPOS PARA LOS QUE EL LOGARITMO DISCRETO ES FÁCIL. CUIDADO

EJ: $(\mathbb{Z}/n\mathbb{Z}\ ,+)$ ← NO ES BUENA ELECCION