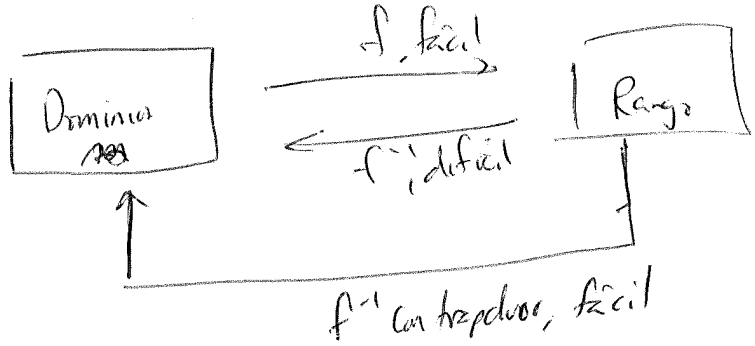
Def (PKC) Un public key cryptosystem consiste de

- one-way functions – una función invertible que es fácil de calcular pero cuyo inverso es difícil de calcular
- trapdoor information – un pedacito de información extra que hace fácil calcular el inverso



En los términos de cifrados asimetricos

$$f = e_{k_{pub}}, \quad f^{-1} = "d_{k_{pub}}"$$

$$f^{-1}, \text{fácil} = "d_{k_{priv}}".$$

No se sabe si ningún one-way function existe.

$$\Updownarrow$$

$$P = NP$$

Def. Sea p un primo (grande), g una raíz primitiva módulo p.

Sea h un elemento no nulo de $\mathbb{F}_p$. El problema del logaritmo discreto (DLP) es el problema de encontrar una potencia x t.q.

$$g^x \equiv h \pmod{p}$$

El número x se llama el logaritmo discreto de h en la base g y se denota $\log_g(h)$.

(!!) **Ojo:** muchas veces se usa el logaritmo en base 2 para medir la complejidad de algoritmos; es fácil confundir $\log_2(\cdot)$ en ese caso.

Obs: Si hay una solución, hay infinitas — Fermat.

entonces se define $\log_g : \mathbb{F}_p^\times \to \mathbb{Z}/(p-1)\mathbb{Z}$.

Obs: $\log_g(ab) = \log_g(a) + \log(b)$ ← convierte multiplicación en suma.

Obs: Se puede generalizar a cualquier grupo G.

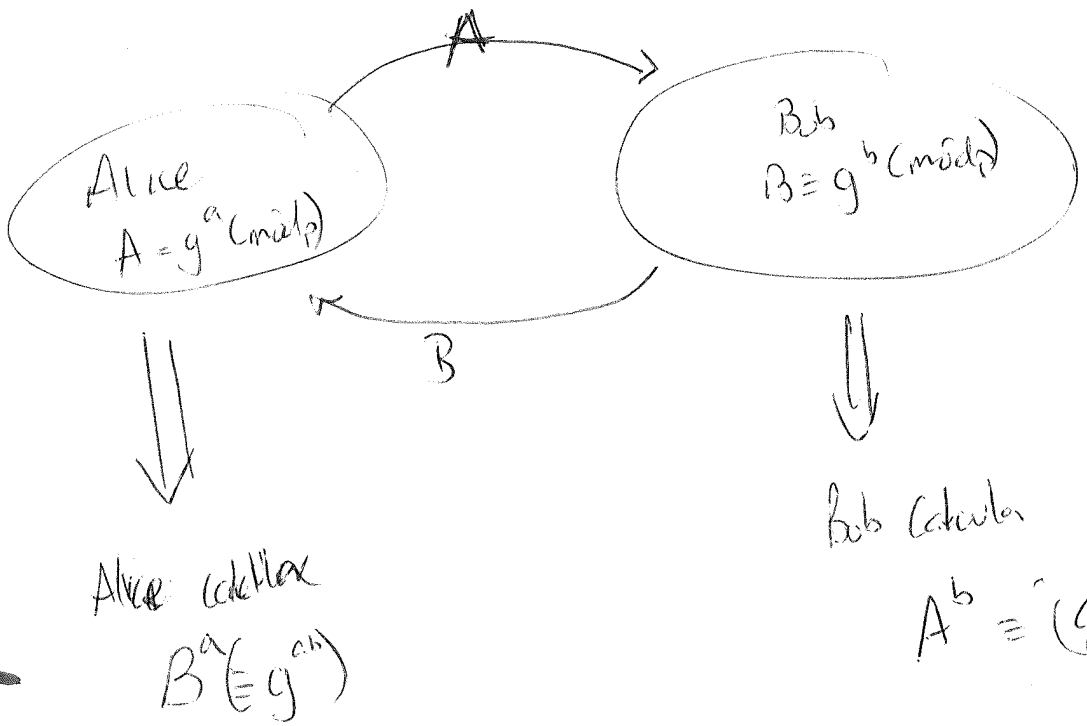
Diffie-Hellman

Alice y Bob eligen un primo grande y un cierto número g no-nulo. Públicamente g y p. Idealmente elegirían un g cuyo orden en $\mathbb{F}_p^\times$ es un primo (grande).

Entonces

Alice elige un a secreto y calcula $A \equiv g^a \pmod p$

Bob elige un b secreto y calcula $B \equiv g^a \pmod p$



Ej: $p = 941$, $g = 627$, $a = 347$, $b = 781$

$A \equiv 390 \pmod{941}$; $B = 691 \pmod{941}$

$A^b \equiv B^a \equiv 470 \pmod{941}$.

Supongamos que Eve monitorea todo el intercambio. Si Eve puede resolver $390 \equiv 627^a \pmod{941}$ o puede resolver $691 \equiv 627^b \pmod{941}$ puede saber la clave.

Se sospecha que es la única manera.

El problema de Eve es:

Sabe ~~$A = g^a$~~ $g, p, A = g^a$ y $B = g^b$.

Hace Si puede resolver el DLP puede romper el sistema.

Pero la seguridad de DH depende de ~~otro problema~~:
la dificultad de otro problema

Def.. p primo, $g \in \mathbb{Z}$. El problema de Diffie Hellman (DHP) es el problem de calcular g^{ab} sabiendo solamente g^a y g^b.

Obs: resolver ~~DLP~~ $\Rightarrow$ resolver DHP.

resolver DHP $\overset{??}{\Rightarrow}$ resolver DLP?
No se sabe.