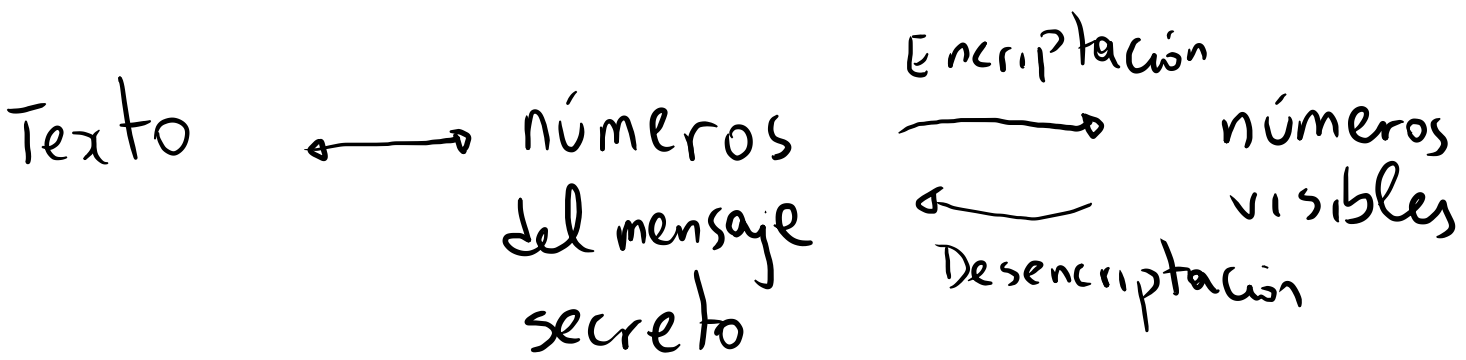


Diffie - Hellman

Dato secreto compartido por A y B
es un número (módulo otro número)

Este número puede usarse como
clave para cambiar números
por otros siguiendo otro método

números secretos

claves para

números del mensaje ⟶ ⟵ números visibles.

Con D-H ó R-S-A creás una clave

y la usás para transformar

entre números secretos y números visibles

ECB

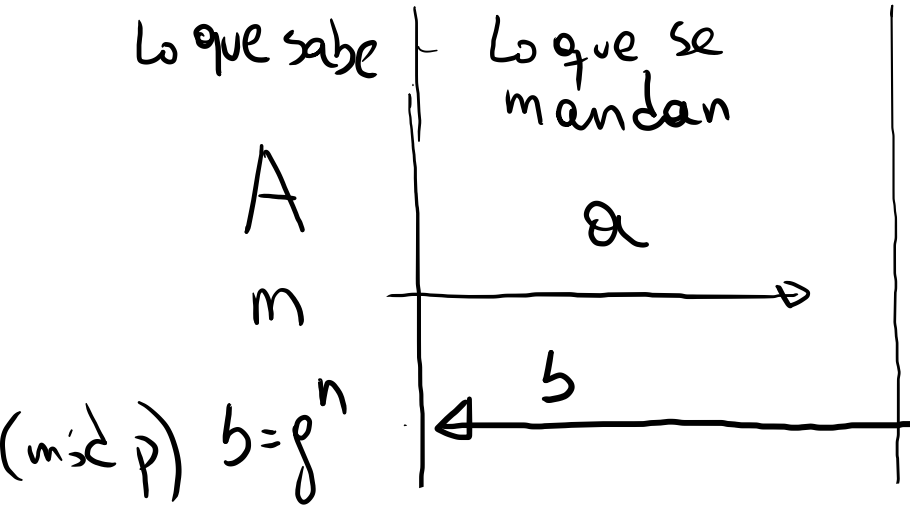
métodos: César

afines

Vigénère

Diffie - Hellman

Datos públicos: p primo, g raíz prim. mód p.

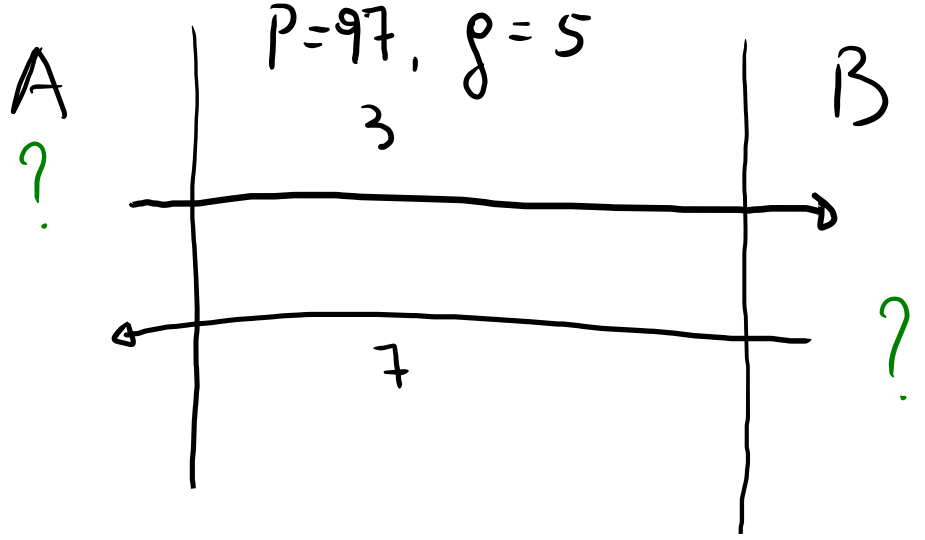


$$b^m = \left(g^n\right)^m = g^{nm} \longleftrightarrow a^n = \left(g^m\right)^n = g^{mn}$$

lo llamamos K

Es re difícil obtener m sabiendo a (logaritmo discreto)
n sabiendo b

35) somos espías m, n son mód



$\varphi(97) = 96$

$g^m \equiv 3$, $g^n \equiv 7$ (mód 97) 1, 5, -1, -5

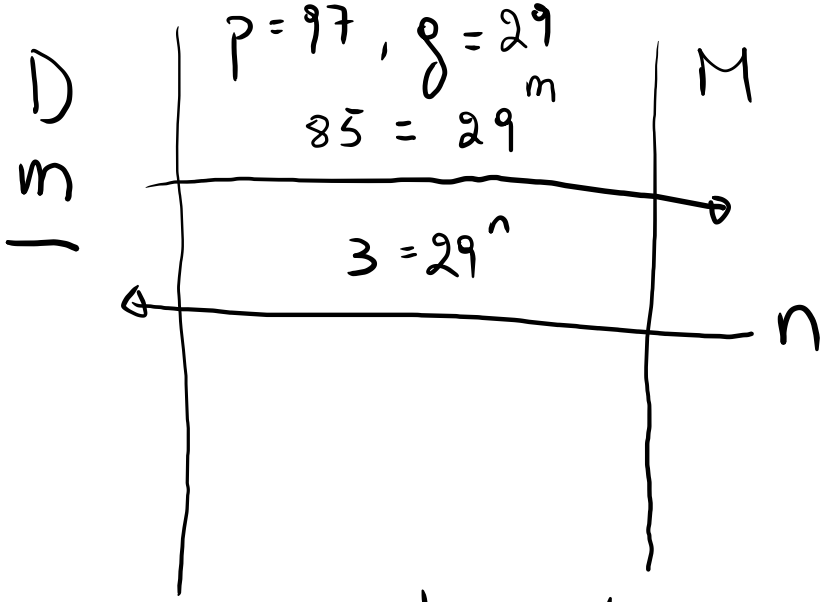
Potencias de 5: (a lo sumo $\frac{96}{2} - 4$) 48 - 4 = 44

5^0 5^1 5^2 5^3 5^4 5^5

1, 5, 25, 125 ≡ 28, 140 ≡ 43, 215 ≡ 21, 105 ≡ 8 ≡ 5^6

multiplicamos por 5

$5^{11} = 5^6 \cdot 5^5 = 8 \cdot 21 = 168 \equiv 71$



(*) $85 = 29^m$ → método D-H

$29 = 5^{13}$ → letra (casualidad que lo sabemos)

Además justo sabíamos que (mód 97)

$\log_5 29 \equiv 13$ $\quad \log_5 85 \equiv 90$

$29 \equiv 5^{13}$

$85 \equiv 5^{90} \overset{(*)}{=} \left(5^{13}\right)^m = 5^{13m}$

$90 \equiv 13m$ mód $\varphi(97) = 96$

Hay que encontrar el inverso de 13 módulo 96., y entonces

$$90 \equiv 13m \pmod{96}$$

$$90x \equiv m \pmod{96}$$

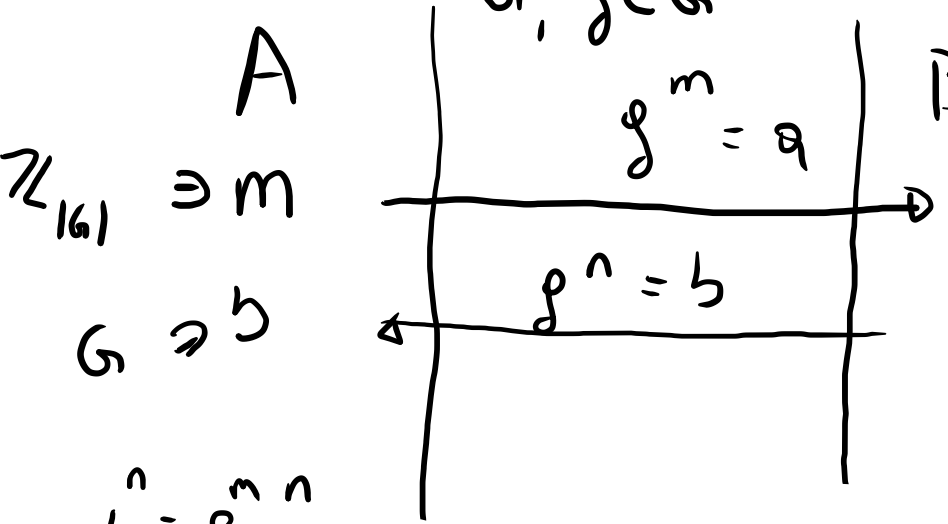
Terminar el ejercicio con lo que ya sabemos

Después de esto vamos a conocer $\underline{m}$

¿Cómo seguimos? Ahora sabemos lo mismo que sabe Diego: $(29^n)^m = 3^m \pmod{97}$ → lo que mandó Marta

Diffie-Hellman generalizado a cualquier grupo (por eso usamos la letra g)

público
G, $g \in G$



En algunos grupos es más difícil hacer log. discreto
$U(p) \rightarrow$ difícil
$\mathbb{Z}_p \rightarrow$ fácil
(15)