

① We want to find $(\alpha, \beta) \in \mathbb{N}^2$ s.t. $g^{\alpha+x} \cdot h^{-(\beta+y)} = g^x \cdot h^{-y} \pmod{p}$.

Let's denote by α' and β' the order of g and h in \mathbb{Z}_p^* , respectively. It means that $g^{\alpha'} = 1 \pmod{p}$ and $h^{\beta'} = 1 \pmod{p}$. We have, for any $(x, y) \in \mathbb{N}^2$,

$$g^{(\alpha'+x)} \cdot h^{-(\beta'+y)} = g^{\alpha'} \cdot g^x \cdot h^{-\beta'} \cdot h^{-y} = (g^{\alpha'} \cdot h^{-\beta'}) g^x \cdot h^{-y} \underset{g^{\alpha'}=1 \pmod{p}}{=} (h^{\beta'})^{-1} \cdot g^x \cdot h^{-y} \underset{h^{\beta'}=1 \pmod{p}}{=} (1)^{-1} \cdot g^x \cdot h^{-y} \pmod{p}.$$

So, the fct. is periodic with period (α', β') .

Given a period (α, β) , you can compute the discrete logarithm. We know that

$$g^{x+\alpha} \cdot h^{-(y+\beta)} = g^x \cdot h^{-y} \pmod{p}. \text{ And this happens } \Leftrightarrow g^{\alpha} \cdot h^{-\beta} = 1 \pmod{p}$$

$$\Leftrightarrow g^{\alpha} = h^{\beta} \pmod{p}$$

$$\Leftrightarrow g^{\alpha} = g^{a\beta} \pmod{p}$$

$$\Leftrightarrow a = \alpha \cdot \beta^{-1} \pmod{q} \text{ where } q \text{ is the order of } g.$$