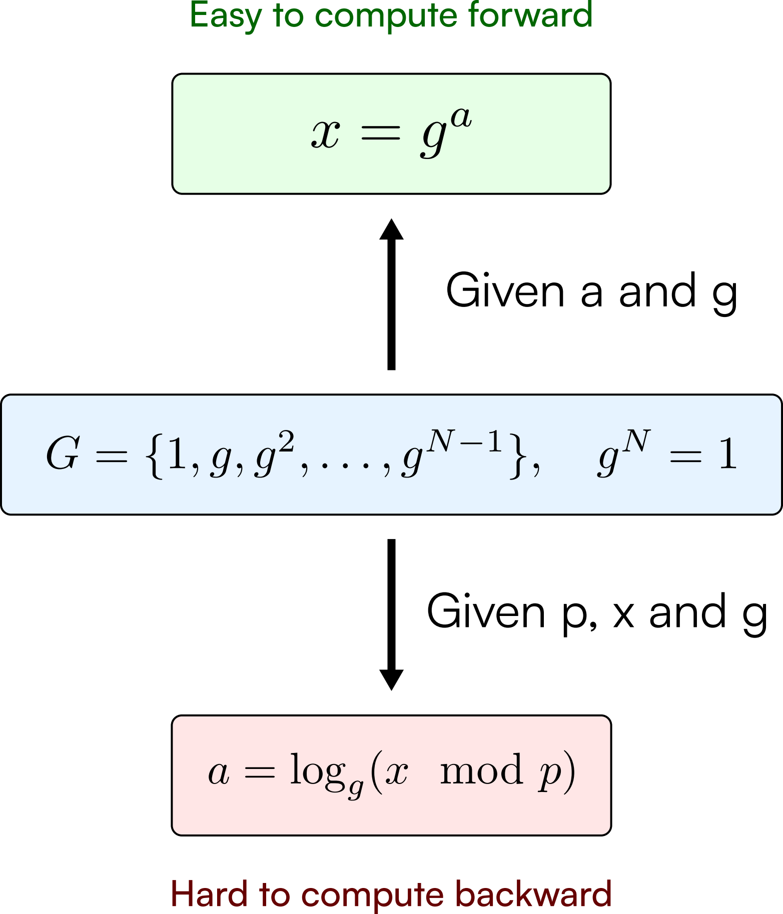

Easy to compute forward

$$x = g^a$$

Given a and g

$$G = \{1, g, g^2, \dots, g^{N-1}\}, \quad g^N = 1$$

Given p, x and g

$$a = \log_g(x \mod p)$$

Hard to compute backward