

§ Discrete Logarithm Problem

In discrete case

$$a^x = b$$

Forward Operation: exponentiation
given a, x , calculate b

Square-and-Multiply

Inverse Operation: discrete logarithm
given a, b , calculate x

Very much brute force

$$a^{\boxed{x}} = \underbrace{a \cdot a \cdots a}_{\boxed{x} \text{ times}} = \boxed{b}$$

