Outline

Discrete Logarithm Problem

Brute force : $O(N)$ steps and $O(1)$ space

Baby-step-Giant-step : $O(\sqrt{N} \log N)$ steps

$O(\sqrt{N})$ space

Discrete Logarithm Problem (DLP)

Given a group G with operation $\cdot$ (written multiplicatively), and its identity element is 1.

Let $g, h \in G$. Find an integer x such that $g^x = h$.

In $\mathbb{Z}_n^*$, the operation is multiplication

given g, h, want to compute x such that

$$g^x = h \bmod n$$

Hard

Hardness of DLP depends on group

In $\mathbb{Z}_n$ with operation $+$, written additively

Given $g, h \in \mathbb{Z}_n$, want to x.

$$x \cdot g = h \mod n$$

To find x,

$$x = h g^{-1} \mod n$$

Easy problem

Brute - Force Method

Given g, h find x s.t $g^x = h \in G$

Successive multiplication of g until we reach h.

Running time: $O(\text{ord}(g))$

$O(|G|)$ exponential in # of bits to store $|G|$

$$|G| = 2^{\log |G|}$$

Trivial Space and Running Time

Given a group G,

$g, h \in G$.

g has order N.

Then there exists an algorithm to solve DLP in $O(N)$ steps and in $O(1)$ space.

each step is group multiplication

Baby-step-Giant-Step

Trade-off time with space

$g^x = h$, $N = \mathrm{ord}(g)$

$x = im + j$ $\quad m = \lceil \sqrt{N} \rceil$

$0 \le i < m$

$0 \le j < m$

Create two lists :

L1 : $g^0, g^1, g^2, \ldots, g^{m-1}$

L2 : $hu^0, hu^1, hu^2, \ldots, hu^{m-1}$

$u = g^{-m}$

Find the matched value g^j , hu^i

$x = im + j$.

$x = im + j$

$g^x = g^{im+j} = h$

$g^j = h g^{-mi}$

$= h u^i$

Running time:

$O(m)$ multiplications

$O(m \log m)$ sorting & finding match

Total $O(m \log m)$

$= O(\sqrt{N} \log \sqrt{N})$

$= O(\sqrt{N} \log N)$ steps

Space $= O(m) = O(\sqrt{N})$

Proposition 2.21 (Shanks's Babystep–Giantstep Algorithm)**.** *Let G be a group and let $g \in G$ be an element of order $N \geq 2$. The following algorithm solves the discrete logarithm problem $g^x = h$ in $\mathcal{O}(\sqrt{N} \cdot \log N)$ steps using $\mathcal{O}(\sqrt{N})$ storage.*

(1) *Let $n = 1 + \lfloor \sqrt{N} \rfloor$, so in particular, $n > \sqrt{N}$.*

(2) *Create two lists,*

$$\begin{aligned} &\text{List 1:} \quad e,\ g,\ g^2,\ g^3, \ldots, g^n, \\ &\text{List 2:} \quad h,\ h \cdot g^{-n},\ h \cdot g^{-2n},\ h \cdot g^{-3n}, \ldots, h \cdot g^{-n^2}. \end{aligned}$$

(3) *Find a match between the two lists, say $g^i = hg^{-jn}$.*

(4) *Then $x = i + jn$ is a solution to $g^x = h$.*