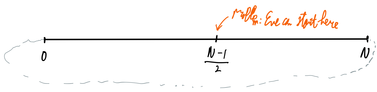
discrete log problem

give: P and P_A, find $a = \log_P P_A$,
i.e. $P_A = aP$

naive method: try $P, 2P, 3P, \ldots$ (notable feature)
assume that P has order N, i.e. $NP = 0$
naive method takes at most $N-1$ additions

Can use $-P = (N-1)P$ symmetry to (i.e. stopping point) succeed in at most $\left\lceil \frac{N-1}{2} \right\rceil$ steps

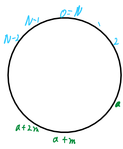
If Eve is known to try $P, 2P, 3P, \ldots$
then always a is safer.
(always as $a \le \frac{N-1}{2}$ if Eve uses symmetry)



Eve can randomize P_A to avoid stuck "collisions"

$P_A + rP$ for random r moves target DLP to $a+r \bmod N$

Eve can "blow up" the single target into 100 targets $P_A + r_1 P$, $P_A + r_2 P$, ... for random r_i;
this improves her chance of finding one in $P, 2P, 3P$



mean. Split interval $[0, N-1]$ into 100 equal pieces. Let $m = \frac{N}{100}$, and find targets
P_A, $P_A + mP$, $P_A + 2mP$, $P_A + 3mP$, ..., $P_A + 99mP$, so that one is at most first $\frac{N}{100} = m$ steps
(mP uses double-and-add method)

if $P_A + rP = cP$ for a c and r we know

(Eve computes $P, 2P, \ldots$, at each step checks against all targets)

Then $aP + rP = cP$, i.e.

$$a \equiv c - r \bmod N$$

The first DLP will be solved in $\frac{N}{100}$.

With 1000 targets, i.e. $m = \frac{N}{1000}$, solve in $\frac{N}{1000}$

With 10^i targets, $m = \frac{N}{10^i}$, solve in $\frac{N}{10^i}$

Warning: the first step takes 10^i computation and 10^i storage.
the second step (compute $P, 2P, \ldots, cP$ and compare to list) takes $\frac{N}{10^i}$ steps.

Do not choose i so large that $\frac{N}{10^i} < 10^i$. Optimal limit is $10^i \le \sqrt{N}$

Storage is more expensive than computation, so limit the steps which incur storage.

This attack is (mostly, apart from swapping phase 1 and 2) the baby-step-giant-step attack.

Baby-step-giant-step attack (BSGS attack)

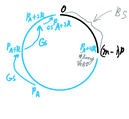
Given P, P_A, and N, $m = \lfloor \sqrt{N} \rfloor$

Baby steps: compute $0P, 1P, 2P, \ldots, (m-1)P$ and store as (iP, i) indexed by iP.

Giant steps: compute $R = mP$.

$j = 0$, $Q = P_A$
while Q not in targets
$j = j + 1$
$Q = Q + R$

output j and i, where we have a match



$P_A + qR = iP$
$aP + qmP = iP$
$a \equiv i - qm \bmod N$
j is good