Discrete logarithm problem

Pohlig–Hellman example

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Example

$y^2 = x^3 - x$ over $\mathbb{F}_p, p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

Example

$y^2 = x^3 - x$ over $\mathbf{F}_p, p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Example

$y^2 = x^3 - x$ over $\mathbf{F}_p, p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S$

Example

$y^2 = x^3 - x$ over $\mathbf{F}_p, p = 1000003$.
$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

Example

$y^2 = x^3 - x$ over $\mathbf{F}_p, p = 1000003$.
$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$

Example

$y^2 = x^3 - x$ over $\mathbb{F}_p, p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

Example

$y^2 = x^3 - x$ over $\mathbb{F}_p, p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S \equiv a \bmod 2$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

Example

$y^2 = x^3 - x$ over $\mathbf{F}_p, p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S \equiv a \bmod 2$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.

Example

$y^2 = x^3 - x$ over $\mathbb{F}_p, p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S \equiv a \bmod 2$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.

Compute $a_2 = \log_R S \equiv a \bmod 53$. This is a DLP in a group of size 53.

Example

$y^2 = x^3 - x$ over $\mathbf{F}_p, p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S \equiv a \bmod 2$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.

Compute $a_2 = \log_R S \equiv a \bmod 53$. This is a DLP in a group of size 53.

Takes more effort than size 2, but much easier than size 500002.

Can use Pollard rho to attack this subgroup problem in $\sqrt{53\pi/2}$ steps.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 \bmod 53,$$
$$a \equiv a_4 \bmod 89,$$

to determine a modulo

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$\begin{aligned} a &\equiv a_1 \bmod 2, \\ a &\equiv a_2 \bmod 53, \\ a &\equiv a_4 \bmod 89, \end{aligned}$$

to determine a modulo $2 \cdot 53 \cdot 89$.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$\begin{aligned} a &\equiv a_1 \bmod 2, \\ a &\equiv a_2 \bmod 53, \\ a &\equiv a_4 \bmod 89, \end{aligned}$$

to determine a modulo $2 \cdot 53 \cdot 89$. Cost: $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2}$.

Note that cost counts steps, ignores computation of R and S.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$\begin{aligned} a &\equiv a_1 \bmod 2, \\ a &\equiv a_2 \bmod 53, \\ a &\equiv a_4 \bmod 89, \end{aligned}$$

to determine a modulo $2 \cdot 53 \cdot 89$. Cost: $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2}$.
Note that cost counts steps, ignores computation of R and S.

But this misses a 53.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$
\begin{aligned}
a &\equiv a_1 \bmod 2,\\
a &\equiv a_2 \bmod 53,\\
a &\equiv a_4 \bmod 89,
\end{aligned}
$$

to determine a modulo $2 \cdot 53 \cdot 89$. Cost: $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2}$.
Note that cost counts steps, ignores computation of R and S.

But this misses a 53. Brute force search in residue class: cost $+53$.

Are we there, yet?

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 89)P$ has order 53^2, and
$S = (2 \cdot 89)Q$ is multiple of R.
Compute $a_5 = \log_R S \equiv a \bmod 53^2$.

Are we there, yet?

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 89)P$ has order 53^2, and
$S = (2 \cdot 89)Q$ is multiple of R.
Compute $a_5 = \log_R S \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_5 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Are we there, yet?

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 89)P$ has order 53^2, and
$S = (2 \cdot 89)Q$ is multiple of R.
Compute $a_5 = \log_R S \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_5 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Cost $1 + \sqrt{53^2\pi/2} + \sqrt{89\pi/2} = 79.24$ instead of
cost $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2} + 53$

Are we there, yet? This is not Pohlig–Hellman

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 89)P$ has order 53^2, and
$S = (2 \cdot 89)Q$ is multiple of R.
Compute $a_5 = \log_R S \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_5 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Cost $1 + \sqrt{53^2\pi/2} + \sqrt{89\pi/2} = 79.24$ instead of
cost $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2} + 53 = 74.94$.

Ratio would look worse without Pollard rho (no square roots):
$1 + 2 \cdot 53 + 89 = 196$ vs $1 + 53^2 + 89 = 2899$.

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T$

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T \equiv a' \bmod 53$.

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T \equiv a' \bmod 53$.
Note $a_2 + 53a_3 \equiv a \bmod 53^2$.

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.
$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T \equiv a' \bmod 53$.
Note $a_2 + 53a_3 \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 + 53a_3 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.
$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T \equiv a' \bmod 53$.
Note $a_2 + 53a_3 \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 + 53a_3 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Cost $1 + 2\sqrt{53\pi/2} + \sqrt{89\pi/2} = 31.07 < 74.94$.

Pohlig–Hellman overview

Pohlig–Hellman attack turns DLP $a = \log_P Q$ in group of order

$$n = \prod p_i^{e_i}, \quad p_i \text{ prime }, p_i \neq p_j, e_i \in \mathrm{Z}_{>0}$$

into

$$\sum (e_i \text{ DLPs in group of order } p_i),$$

$\sum(e_i + 1)$ scalar multiplications, and one application of the CRT.

Pohlig–Hellman overview

Pohlig–Hellman attack turns DLP $a = \log_P Q$ in group of order

$$n = \prod p_i^{e_i}, \quad p_i \text{ prime }, p_i \neq p_j, e_i \in \mathrm{Z}_{>0}$$

into

$$\sum (e_i \text{ DLPs in group of order } p_i),$$

$\sum(e_i + 1)$ scalar multiplications, and one application of the CRT.

Examples: $n \in \{61, 63, 64, 65\}$

- $n = 64$: 7 scalar multiplications (by 32), 16, 8, 4, 2, 1), 6 trivial DLs.
- $n = 61$: 1 DL in group of 61 elements (no effect of PH).

Pohlig–Hellman overview

Pohlig–Hellman attack turns DLP $a = \log_P Q$ in group of order

$$n = \prod p_i^{e_i}, \quad p_i \text{ prime }, p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$$

into

$$\sum (e_i \text{ DLPs in group of order } p_i),$$

$\sum(e_i + 1)$ scalar multiplications, and one application of the CRT.

Examples: $n \in \{61, 63, 64, 65\}$

- $n = 64$: 7 scalar multiplications (by 32), 16, 8, 4, 2, 1), 6 trivial DLs.
- $n = 61$: 1 DL in group of 61 elements (no effect of PH).
- $n = 65 = 5 \cdot 13$: 4 scalar multiplications (by 13 and 5), 1 DL in group of 5 elements, 1 DL in group of 13 elements.
- $n = 63 = 3^2 \cdot 7$: 5 scalar multiplications (by 21, 7, and 9), 2 DLs in group of 3 elements, 1 DL in group of 7 elements.

Pohlig–Hellman overview

Pohlig–Hellman attack turns DLP $a = \log_P Q$ in group of order

$$n = \prod p_i^{e_i}, \quad p_i \text{ prime }, p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$$

into

$$\sum (e_i \text{ DLPs in group of order } p_i),$$

$\sum (e_i + 1)$ scalar multiplications, and one application of the CRT.

Examples: $n \in \{61, 63, 64, 65\}$

- $n = 64$: 7 scalar multiplications (by 32), 16, 8, 4, 2, 1), 6 trivial DLs.
- $n = 61$: 1 DL in group of 61 elements (no effect of PH).
- $n = 65 = 5 \cdot 13$: 4 scalar multiplications (by 13 and 5), 1 DL in group of 5 elements, 1 DL in group of 13 elements.
- $n = 63 = 3^2 \cdot 7$: 5 scalar multiplications (by 21, 7, and 9), 2 DLs in group of 3 elements, 1 DL in group of 7 elements.

Pohlig-Hellman method reduces security of discrete logarithm problem in group generated by P to security of largest prime order subgroup.

Many groups are much weaker than their size n predicts!

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbb{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.
$S_i = n_i Q$ is multiple of R_i, i.e., $S_i = a_i R_i$, where $a_i \equiv a \bmod p_i$.

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.
$S_i = n_i Q$ is multiple of R_i, i.e., $S_i = a_i R_i$, where $a_i \equiv a \bmod p_i$.
Solve this problem with an appropriate method,
i.e., brute force for tiny p_i, BSGS or Pollard rho for bigger ones.

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.
$S_i = n_i Q$ is multiple of R_i, i.e., $S_i = a_i R_i$, where $a_i \equiv a \bmod p_i$.
Solve this problem with an appropriate method,
i.e., brute force for tiny p_i, BSGS or Pollard rho for bigger ones.

If $e_i = 1$ we are done.

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.
$S_i = n_i Q$ is multiple of R_i, i.e., $S_i = a_i R_i$, where $a_i \equiv a \bmod p_i$.
Solve this problem with an appropriate method,
i.e., brute force for tiny p_i, BSGS or Pollard rho for bigger ones.

If $e_i = 1$ we are done.
Else we need to do $e_i - 1$ more steps of the same hardness.

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.
$S_i = n_i Q$ is multiple of R_i, i.e., $S_i = a_i R_i$, where $a_i \equiv a \bmod p_i$.
Solve this problem with an appropriate method,
i.e., brute force for tiny p_i, BSGS or Pollard rho for bigger ones.

If $e_i = 1$ we are done.
Else we need to do $e_i - 1$ more steps of the same hardness.

Each of these steps updates n_i to n_i/p_i, does not touch R_i
(we solve another DLP in the group of order p_i generated by R_i),
and updates target S_i:

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.
$S_i = n_i Q$ is multiple of R_i, i.e., $S_i = a_i R_i$, where $a_i \equiv a \bmod p_i$.
Solve this problem with an appropriate method,
i.e., brute force for tiny p_i, BSGS or Pollard rho for bigger ones.

If $e_i = 1$ we are done.
Else we need to do $e_i - 1$ more steps of the same hardness.

Each of these steps updates n_i to n_i/p_i, does not touch R_i
(we solve another DLP in the group of order p_i generated by R_i),
and updates target S_i:

Assume $e_i = 2$:
We want new $S_i = n_i Q$ to be multiple of R_i,

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.
$S_i = n_i Q$ is multiple of R_i, i.e., $S_i = a_i R_i$, where $a_i \equiv a \bmod p_i$.
Solve this problem with an appropriate method,
i.e., brute force for tiny p_i, BSGS or Pollard rho for bigger ones.

If $e_i = 1$ we are done.
Else we need to do $e_i - 1$ more steps of the same hardness.

Each of these steps updates n_i to n_i/p_i, does not touch R_i
(we solve another DLP in the group of order p_i generated by R_i),
and updates target S_i:

Assume $e_i = 2$:
We want new $S_i = n_i Q$ to be multiple of R_i, but n_i lost an extra p_i and unless $a_i = 0$ in previous step we need to update Q to Q'.

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathrm{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.
$S_i = n_i Q$ is multiple of R_i, i.e., $S_i = a_i R_i$, where $a_i \equiv a \bmod p_i$.
Solve this problem with an appropriate method,
i.e., brute force for tiny p_i, BSGS or Pollard rho for bigger ones.

If $e_i = 1$ we are done.
Else we need to do $e_i - 1$ more steps of the same hardness.

Each of these steps updates n_i to n_i/p_i, does not touch R_i
(we solve another DLP in the group of order p_i generated by R_i),
and updates target S_i:

Assume $e_i = 2$:
We want new $S_i = n_i Q'$ to be multiple of R_i, but n_i lost an extra p_i and unless $a_i = 0$ in previous step we need to update Q to Q'.

Handling of one prime power I

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbb{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.
$S_i = n_i Q$ is multiple of R_i, i.e., $S_i = a_i R_i$, where $a_i \equiv a \bmod p_i$.
Solve this problem with an appropriate method,
i.e., brute force for tiny p_i, BSGS or Pollard rho for bigger ones.

If $e_i = 1$ we are done.
Else we need to do $e_i - 1$ more steps of the same hardness.

Each of these steps updates n_i to n_i/p_i, does not touch R_i
(we solve another DLP in the group of order p_i generated by R_i),
and updates target S_i:

Assume $e_i = 2$:
We want new $S_i = n_i Q'$ to be multiple of R_i, but n_i lost an extra p_i and unless $a_i = 0$ in previous step we need to update Q to Q'.
$S_i = n_i(Q - a_i P) = n_i(a - a_i)P = n_i(p_i a')P = a' R_i$.

Handling of one prime power II

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Handling of one prime power II

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbb{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.

Let $a_i = a_{i,0} + a_{i,1}p_i + a_{i,2}p_i^2 + \cdots + a_{i,e_i-1}p_i^{e_i-1}$ and $a \equiv a_i \bmod p_i^{e_i}$.

We first compute $a_{i,0}$, then $a_{i,1}, a_{i,2}, \ldots$
Note $a_i - (a_{i,0} + a_{i,1}p_i) = a_{i,2}p_i^2 + \cdots + a_{i,e_i-1}p_i^{e_i-1}$ is multiple of p_i^2.

Handling of one prime power II

Let $n = \prod p_i^{e_i}$, for p_i prime, $p_i \neq p_j, e_i \in \mathbb{Z}_{>0}$.
This slide handles $p_i^{e_i}$ for one prime p_i; repeat to get all primes.

Put $n_i = n/p_i$. P has order n.
$R_i = n_i P$ has order p_i.

Let $a_i = a_{i,0} + a_{i,1}p_i + a_{i,2}p_i^2 + \cdots + a_{i,e_i-1}p_i^{e_i-1}$ and $a \equiv a_i \bmod p_i^{e_i}$.

We first compute $a_{i,0}$, then $a_{i,1}, a_{i,2}, \ldots$
Note $a_i - (a_{i,0} + a_{i,1}p_i) = a_{i,2}p_i^2 + \cdots + a_{i,e_i-1}p_i^{e_i-1}$ is multiple of p_i^2.

In general $a_i - (a_{i,0} + a_{i,1}p_i + \cdots + a_{i,j-1}p_i^{j-1}) = a_{i,j}p_i^j + \cdots + a_{i,e_i-1}p_i^{e_i-1}$ is multiple of p_i^j.

Initialize $Q_i = Q$ and $a_{i,-1} = 0$. (So that all steps look the same).

The jth of the e_i steps, for $0 \leq j < e_i$:

- updates n_i to n_i/p_i and Q_i to $Q_i - a_{i,j-1}p_i^{j-1}P$;
  n_i looses factor p_i, Q_i gains an extra factor of p_i.
- computes $S_i = n_i Q_i$, a multiple of R_i, i.e., $S_i = a_{i,j}R_i$, using the new n_i and Q_i;
- solves this DLP to get $a_{i,j}$.

Pohlig–Hellman attack

Input: points P, Q with $Q = aP$, order $n = \prod_{i=1}^{r} p_i^{e_i}$ of P
with $p_i \neq p_j, e_i \in \mathbf{Z}_{>0}$, fully factored

Output: discrete logarithm a of Q base P

1. for $i = 1$ to r
   - 1.1 put $Q_i = Q$, $a_{i,-1} = 0, n_i = n/p_i$
   - 1.2 compute $R_i = n_i P$
   - 1.3 for $j = 0$ to $e_i - 1$
     - 1.3.1 compute $n_i = n/p_i^{j+1}$ # divide old n_i by p_i unless $j = 0$
     - 1.3.2 compute $Q_i = Q_i - (a_{i,j-1} p_i^{j-1})P$
     - 1.3.3 compute $S_i = n_i Q_i$
     - 1.3.4 solve DLP $S_i = a_{i,j} R_i$ of order p_i
   - 1.4 compute $a_i = \sum_{j=0}^{e_j - 1} a_{i,j} p_i^j$
2. solve CRT

$$\begin{aligned} a &\equiv a_1 \bmod p_1^{e_1} \\ a &\equiv a_2 \bmod p_2^{e_2} \\ &\vdots \\ a &\equiv a_r \bmod p_r^{e_r} \end{aligned}$$

   to get $a \bmod n$

CRT works because $p_i^{e_i}$ are coprime and have product n.