Babystep-Giantstep algorithm
THE PROOF

Babystep-Giantstep Algorithm

PROOF

$$n = [\sqrt{N}] + 1 > \sqrt{N} \Rightarrow n^2 > N$$

1) Assume a matching exists.

SHANK'S BABYSTEP-GIANTSTEP ALGORITHM

Let $p > 2$ be a prime, $g \in \mathbb{F}_p^*$ of order $\leq N < p$ and $h \in \mathbb{F}_p^*$.

1. Let $n = 1 + [\sqrt{N}]$;
2. Create two n-lists.

   List 1: $1, g, g^2, ..., g^{n-1}$ List 2: $h, hg^{-n}, h(g^{-n})^2, ..., h(g^{-n})^{n-1}$
3. A match between the two lists exists iff $g^x = h$ has a solution;
4. If $g^i = hg^{-jn}$ for $1 \leq i, j \leq n$, then $x = i + jn$ solves $g^x = h$.

2) Assume $g^x = h$ is solvable. Existence of a match:

Babystep-Giantstep Algorithm

PROOF

When solvable, the DLP $g^x = h$ take $O(\sqrt{N}\log N)$ steps, $O(\sqrt{N})$ storage.

3) Number of elementary operations:

- **Lists 1 and 2:**

$$2n \text{ products mod } p$$

$$(g^n)^{-1} \text{ mod } p$$

$$n \text{ products by } h \text{ mod } p$$

- **Step 3: Matching: need to sort.**

Unit 5
Pohlig-Hellman Algorithm

Recall: an algorithm for finding a primitive root:

ALGORITHM Let $p > 2$ be prime and $p - 1 = \prod_{i=1}^{m} p_i^{a_i}$ be the prime decomposition of $p - 1$, with p_i distinct and $a_i \geq 1$ for $i = 1, \ldots, m$.

1. $g = 2$.
2. If $g^{(p-1)/p_i} \not\equiv 1$ for all $i = 1, \ldots, m$ then g is a primitive root.
3. If not, back to Step 2 with $g \to g + 1$.

What count here are the primes of the decomposition of $p - 1$, not their multiplicities.

Order and DLP

REMARK **Let $p > 2$ be a prime. Let $g \in \mathbb{F}_p^*$.**

1. **The lower is $\mathrm{ord}_p(g)$ the easier is to solve $\log_g$ problem:**

   there are $\mathrm{ord}_p(g)$ distinct values in $\mathbb{F}_p$ for $g^i, i \in \mathbb{N}$.

2. **For every $n \mid p-1$, $\mathrm{ord}_p(g^{(p-1)/n}) \mid n$, in particular $\mathrm{ord}_p(g^{(p-1)/n}) \leq n$.**

Pohlig-Hellman Algorithm

THEOREM (Pohlig-Helman algorithm) NEEDS A FACTORIZATION INTO PRIMES

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$

   admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i [p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$(*) \qquad x \equiv y_1 [p_1^{a_1}], \quad x \equiv y_2 [p_2^{a_2}], \quad \ldots, \quad x \equiv y_m [p_m^{a_m}].$$

solvable with the Chinese Remainder Theorem

REMARK Since $\mathrm{ord}_p(g_i) \mid p_i^{a_i}$, if $(*)$ holds then $g_i^x \equiv g_i^{y_i} [p]$.

Pohlig-Hellman Algorithm

WARNING: AVOID CONFUSIONS

REMARK

1. **Do not confuse the strategy with one for the algorithm for checking whether $g \in \mathbb{F}_p^*$ is a primitive root.**

   - **Check for g being a primitive root: one needs to compute $g^{(p-1)/p_i}$**
   - **Poligh - Hellman: we compute $g^{(p-1)/p_i^{a_i}}$.**

2. **Do not confuse with the BGA: we require here that $\mathrm{ord}_p(g) \mid N$,**

   not just that $\mathrm{ord}_g(p) \leq N$ as in BGA.

Pohlig-Hellman Algorithm

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$ admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.
2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

EXAMPLE Solve $2^x \equiv 7[13]$.

$N = 13 - 1 = 12 = 2^2 \cdot 3.$

Step 1.

Step 2. Solve

Check:

Pohlig-Hellman Algorithm

EXAMPLE $p = 37, g = 2$. We want to solve $g^x = 14$ in $\mathbb{F}_{37}$. $p - 1 = 36 = 2^2 \cdot 3^2$.

APPROXIMATE COMPARISON OF THE METHODS: Babystep-Giantstep vs Pohlig-Hellman [count 1 for each sum/product or power mod p, 1 for inverse, 1 for Ext. Euclidean algebra]

- Naive method:
- Babystep-Giantstep:
- Poligh-Hellman:

We do not care about sorting

POHLIG-

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$ admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.
2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

3. 2×2 Chinese RT:

Pohlig-Hellman Algorithm

EXAMPLE $p = 37, g = 2$. We want to solve $g^x = 14$ in $\mathbb{F}_{37}$.

$p - 1 = 36 = 2^2 \cdot 3^2$. We take $N = 37 - 1$.

Step 1

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\text{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$

   admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

Pohlig-Hellman Algorithm

Step 2

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$

   admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

Pohlig-Hellman Algorithm

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$ admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.
2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

EXAMPLE

Solve $12251^x = 12060$ in $\mathbb{F}_{17681}$.

$$p = 17681,\ N = \mathrm{ord}_p(12251) = 680 = 2^3 \cdot 5 \cdot 17 \quad g = 12251, h = 12060$$

★ $g_1 = 12251^{680/2^3} = 12251^{85} \equiv$
$h_1 = 12060^{680/2^3} = 12060^{85} \equiv$

Solve $g_1^{y_1} = h_1$ in $\mathbb{F}_{17681}$

★ $g_3 = 12251^{680/17} = 12251^{40} \equiv$
$h_3 = 12060^{680/17} = 12060^{40} \equiv$

Solve $g_3^{y_3} = h_3$ in $\mathbb{F}_{17681}$

★ $g_2 = 12251^{680/5} = 12251^{136} \equiv$
$h_2 = 12060^{680/5} = 12060^{136} \equiv$

Solve $g_2^{y_2} = h_2$ in $\mathbb{F}_{17681}$

Pohlig-Hellman Algorithm

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$

   admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

EXAMPLE

Solve $12251^x = 12060$ in $\mathbb{F}_{17681}$.

$$p = 17681,\ N = \mathrm{ord}_p(12251) = 680 = 2^3 \cdot 5 \cdot 17 \quad g = 12251, h = 12060$$

★

Pohlig-Hellman Algorithm

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$

   admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

Pohlig-Hellman Algorithm

We now solve

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$ admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

Pohlig-Hellman Algorithm

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$

   admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

Recall: Pohlig-Hellman Algorithm

THEOREM (Pohlig-Hellman algorithm) NEEDS A FACTORIZATION INTO PRIMES

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$

   admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i [p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$(*) \qquad x \equiv y_1 [p_1^{a_1}], \quad x \equiv y_2 [p_2^{a_2}], \quad \ldots, \quad x \equiv y_m [p_m^{a_m}].$$

solvable with the Chinese Remainder Theorem

Proof of Pohlig-Hellman Algorithm

Proof of Pohlig-Hellman Algorithm

PROOF (N with just 2 distinct primes).

$$N = p_1^{a_1} p_2^{a_2}$$

If $g^x = h$ then

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$ admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.
2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

Conversely let y_i be such that 1) holds: $g_i^{y_i} \equiv h_i[p]$, $i = 1, 2$.

Proof of Pohlig-Hellman Algorithm

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$

   admits a solution iff there are y_i $(i = 1, ..., m)$: $g_i^{y_i} \equiv h_i[p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1[p_1^{a_1}], \quad x \equiv y_2[p_2^{a_2}], \quad \ldots, \quad x \equiv y_m[p_m^{a_m}].$$

Unit 6
Complexity of the Pohlig-Hellman Algorithm

ROUGH COMPARISON OF THE METHODS

the case of p-1 product of small primes

EXAMPLE **Solve $g^x = 12060$ in $\mathbb{F}_{17681}$, g primitive root.** $p = 17681$, $p - 1 = 17680$

$$= 2^4 \times 5 \times 13 \times 17$$

APPROXIMATE COMPARISON OF THE METHODS: Babystep-Giantstep vs Pohlig-Hellman
[count 1 for each sum/product or power mod p, 1 for inverse, 1 for Ext. Euclidean algebra, do not consider sorting]

- **Naive method:**
- **Babystep-Giantstep:**
- **Pohlig-Hellman:**
  1. **Solve DLP for orders $2^4, 5, 13, 17$:**
  2. **3×3 Chinese RT:**

ROUGH COMPARISON OF THE METHODS

the case of p-1 with a large prime factor

EXAMPLE $p = 20000159, p - 1 = 2 \cdot 10000079 + 1$ (10000079 is prime)

Solve $7^x = 11827860[p]$. (7 is a primitive root)

$n = [\sqrt{20000158}] + 1 = 4473.$

APPROXIMATE COMPARISON OF THE METHODS: Babystep-Giantstep vs Pohlig-Hellman
[count 1 for each sum/product or power mod p, 1 for inverse, 1 for Ext. Euclidean algebra, do not consider sorting]

- Naive method:
- Babystep-Giantstep:

- Pohlig-Hellman:
  1. Solve DLP for orders $2, 10000079$:
  2. 2×2 Chinese RT...

Complexity of the Pohlig-Hellman Algorithm

PROPOSITION **Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$,**

$$N = N(p_1, ..., p_m, a_1, ..., a_m) = p_1^{a_1} \cdots p_m^{a_m}.$$

The DLP $g^x = h$ can be solved in $O\left(\sum_{i=1}^{m} a_i p_i\right)$ steps as $N \to +\infty$.

NEEDS A FACTORIZATION INTO PRIMES

REMARK $$\log N \leq \sum_{i=1}^{m} a_i p_i \to +\infty \text{ as } N \to +\infty.$$

Complexity of the Pohlig-Hellman Algorithm

PROPOSITION Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N = p_1^{a_1} \cdots p_m^{a_m}$.

The DLP $g^x = h$ can be solved in $O\left(\sum_{i=1}^{m} a_i p_i\right)$ steps as $N \to +\infty$.

EXAMPLE (small prime) $N = N(a_1) = 2^{a_1}$.

EXAMPLE (small primes) $N = N(a_1, a_2) = 2^{a_1} 7^{a_2}$.

Complexity of the Pohlig-Hellman Algorithm

PROPOSITION Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N = p_1^{a_1} \cdots p_m^{a_m}$.

The DLP $g^x = h$ can be solved in $O\left(\sum_{i=1}^{m} a_i p_i\right)$ steps as $N \to +\infty$.

EXAMPLE [small primes] $N = p_1^{a_1} \cdots p_m^{a_m}$ with $p_i \leq R$ for all i.

The DLP is not secure if $p - 1$ is a product of powers of small primes.

Complexity of the Pohlig-Hellman Algorithm

PROPOSITION Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N = p_1^{a_1} \cdots p_m^{a_m}$.

The DLP $g^x = h$ can be solved in $O\left(\sum_{i=1}^{m} a_i p_i\right)$ steps as $N \to +\infty$.

EXAMPLE (large primes)

EXPONENTIAL

$$N = N(q) = 2q, \text{ with } q \text{ prime.}$$

EXAMPLE (large primes) **EXPONENTIAL**

$$N = N(p_1, ..., p_m, a_1, ..., a_m) = p_1^{a_1} \cdots p_m^{a_m} \text{ with } p_1 \geq N/C \text{ for some } C > 0.$$

Proof of the Complexity of the Pohlig-Hellman Algorithm

PROPOSITION Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$,

$$N = N(p_1, \ldots, p_m, a_1, \ldots, a_m) = p_1^{a_1} \cdots p_m^{a_m}.$$

The DLP $g^x = h$ can be solved in $O\left(\sum_{i=1}^{m} a_i p_i\right)$ steps as $N \to +\infty$.

NOTATION S_N: number of steps needed to solve $g^x = h$ when $\mathrm{ord}_p(g) = N$.

Proof. i) The case $N = q^a$ for some prime q and $a \geq 1$.

$$S_{q^a} =$$

Complexity of the Pohlig-Hellman Algorithm

PROPOSITION Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N = p_1^{a_1} \cdots p_m^{a_m}$.

The DLP $h^x = h$ can be solved in $O\Big(\sum_{i=1}^{m} a_i p_i\Big)$ steps.

ii) The general case.

RECALL: POLIGH-HELLMAN

Let $p > 2$ be prime and $g, h \in \mathbb{F}_p^*$, $\mathrm{ord}_p(g) \mid N$ (example: $N = p - 1$).

Let $N = p_1^{a_1} \cdots p_m^{a_m}$ be the prime decomposition of N, with $a_i \geq 1$ and p_i distinct.

1. For each $1 \leq i \leq m$ let $g_i = g^{N/p_i^{a_i}}, h_i = h^{N/p_i^{a_i}}$. The DLP $g^x = h$ in $\mathbb{F}_p$

   admits a solution iff there are y_i $(i = 1, ..., m)$: $\quad g_i^{y_i} \equiv h_i [p]$.

2. In this case a solution to $g^x \equiv h[p]$ is any x such that

$$x \equiv y_1 [p_1^{a_1}], \quad x \equiv y_2 [p_2^{a_2}], \quad \ldots, \quad x \equiv y_m [p_m^{a_m}].$$

END of Lesson 7
Discrete Logarithms and Diffie-Hellman key exchange