Computational Number Theory Final Problems

Pohlig-Hellman, Baby-step-giant-step

Pohlig-Hellman Example

- DL problem: Find x, s.t., $g^x = h$, in cyclic G, $|G| = q$, given G, q, h, g
- Used when q is ``smooth'' (breaks up into small primes)
- Let Z_{31}^* be a cyclic group Find x, s.t., $3^x = 26$ in Z_{31}^*
- Solution:
- $|Z_{31}^*| = 30$
- Let $q = 30 = 5*3*2$

P-H Example

- Use this fact:
- $(g^{q/qi})^x = (g^x)^{q/qi} = h^{q/qi}\ \forall\ i \in 1..k$
- where $q = \prod_{i=1}^{k} q_i$, where $\{q_i\}$ are the co-prime factors of q

- Basically:
  - Find discrete logs in k smaller groups: order $\{q_i\}$
  - Combine everything using reverse-extended-CRT

P-H Example

- H_1:

- $(g^{30/5})^{x1} \bmod 31 = h^{30/5} \bmod 31$
- $(3^6)^{x1} \bmod 31 = 26^6 \bmod 31$

- $(3^6)^{x1} \bmod 31 = (729 \bmod 31)^{x1} = 16^{x1}$

- $26^6 \bmod 31 = ((26^3 \bmod 31) * (26^3 \bmod 31)) \bmod 31$
  $= (1 * 1) \bmod 31$
  $= 1$
- So, $16^{x1} \equiv 1 \pmod{31}$

Use mod. multiply property to split up exponents as they grow larger

P-H Example

- H_2:

- $(g^{30/3})^{x2} \bmod 31 = h^{30/3} \bmod 31$
- $(3^{10})^{x2} \bmod 31 = 26^{10} \bmod 31$

- $(3^{10})^{x2} \bmod 31 = (59049 \bmod 31)^{x2} = 25^{x2}$
- $26^{10} \bmod 31 = ((26^5 \bmod 31) * (26^5 \bmod 31)) \bmod 31$
  $= (6 * 6) \bmod 31$
  $= 5$
- So, $25^{x2} \equiv 5 \pmod{31}$

P-H Example

- H_3:

- $(g^{30/2})^{x3} \bmod 31 = h^{30/2} \bmod 31$
- $(3^{15})^{x3} \bmod 31 = 26^{15} \bmod 31$

- $(3^{15})^{x3} \bmod 31 = (14348907 \bmod 31)^{x3} = 30^{x3}$
- $26^{15} \bmod 31 = ((26^5 \bmod 31) * (26^5 \bmod 31) * (26^5 \bmod 31)) \bmod 31$

  $= (6 * 6 * 6) \bmod 31$

  $= 30$
- So, $30^{x3} \equiv 30 \pmod{31}$

P-H Example

- We know $|H_1| = q_1 = 5$, $|H_2| = q_2 = 3$, $|H_3| = q_3 = 2$

- Use extended CRT:

$$x = [(x_1 \bmod q_1), (x_2 \bmod q_2), \ldots, (x_k \bmod q_k)]$$
$$\forall\, i \in 1 \ldots k \text{ (k is no. of subgroups)}$$

- We get:
- $x = [(16^{x1} \equiv 1 \pmod{31}), (25^{x2} \equiv (5 \bmod 31)), (30^{x3} \equiv 30 \pmod{31})]$
- Solving, $x = [(0 \bmod 5), (2 \bmod 3), (1 \bmod 2)]$
- Solving, $x = 5$

- Sanity check: $3^5 \bmod 31 = 26$

Baby-Step-Giant-Step Example

- DL problem: Find x, s.t., $g^x = h$, in cyclic G, $|G| = q$, given G, q, h, g

- Used in general case: smooth or ``un-smooth'' q

- Basic idea:
- First, ``cut'' the group into intervals of size t, $t \approx \lfloor \sqrt{q} \rfloor$ — ``giant'' steps''
- Compute points at intervals: $g^0, g^t, g^{2t}, \ldots, g^{\lfloor q/t \rfloor * t}$

BSGS Example

- Second, compute t elements: $h^* g^1$, $h^* g^2$, … $h^* g^t$ – ``baby'' steps

- Third, find an $h^* g^i \stackrel{?}{=} g^{k^*t}$ (for some k > 1)

- Fourth, compute $\log_g h = (k^*t - i) \bmod q$

BSGS Example

- Let Z_{29}^* be a cyclic group Find x, s.t., $2^x = 17$ in Z_{29}^*

- Solution:
- $|Z_{29}^*| = 28$, set cutoff-interval $t \approx \lfloor \sqrt{q} \rfloor \approx 5$, $g = 2$, $h = 17$

- Giant steps:
  - $2^0 \bmod 29 = 1$, $2^5 \bmod 29 = 3$, $2^{10} \bmod 29 = 9$, $2^{15} \bmod 29 = 27$, $2^{20} \bmod 29 = 23$, $2^{25} \bmod 29 = 11$

BSGS Example

- Baby steps:
  - $h = 17$, $g = 2$, so
  - $17 * 2^1 \bmod 29 = 5$,
  - $17 * 2^2 \bmod 29 = 10$,
  - $17 * 2^3 \bmod 29 = 20$,
  - $17 * 2^4 \bmod 29 = 11$,
  - $17 * 2^5 \bmod 29 = 22$

- Now, we need to find $h * g^i \stackrel{?}{=} g^{k*t}$ (for some $k > 1$)
- $17 * 2^4 = 11 = 2^{25}$

Basically, just find a ``match'' between baby and giant steps

BSGS Example

- Finally, compute $\log_g h = (k*t - i) \bmod q$
- $\log_2 17 = (25 - 4) \bmod 28$
- So, $x = 21$

- Sanity check: $2^{21} \bmod 29 = 17$