Announcements

- Next Problem Set groups are up
  Start meeting this week to discuss problems

- Motivation for today:
  - Can use brute force to solve the DLP $g^x \equiv h \mod p$ to break DHKE
  - If $N = \text{ord}(g)$, brute force is $\mathcal{O}(N)$
  - This is not computationally feasible for large values of N
  - We'll look at a *collision algorithm*, Shank's Babystep-Giantstep
    Algorithm works for any group, not just $\mathbb{F}_p^*$
    e.g. We'll see it can apply to elliptic curves later in the semester

Shank's Babystep-Giantstep Algorithm

Let G be a group and $g \in G$ of order $N \geq 2$.

The following algorithm solves the DLP $g^x = h$ in $\mathcal{O}(\sqrt{N} \cdot \log(N))$ using $\mathcal{O}(\sqrt{N})$ storage.

1. Let $n = 1 + \lfloor \sqrt{N} \rfloor$. Note $n > \sqrt{N}$
2. Create two lists:
   List 1: $e, g, g^2, g^3, \ldots, g^n$ *(the baby steps)*
   List 2: $h, h \cdot g^{-n}, h \cdot g^{-2n}, h \cdot g^{-3n}, \ldots, h \cdot g^{-n^2}$ *(the giant steps)*
3. Find a match between the two lists, say $g^i = hg^{-jn}$
4. Then $x = i + jn$ is a solution to $g^x = h$

Example: $2^x \equiv 21 \mod 29$

$p = 29$, $g = 2$, $h = 21$, $N = \text{ord}(g) = 28$ (via Mathematica)

$n =$

Example: $2^x \equiv 21 \mod 29$

$p = 29$, $g = 2$, $h = 21$, $N = \text{ord}(g) = 28$ (via Mathematica)

$n =$

	i/j	0	1	2	3	4	5	6
Babysteps	2^i							
Giantsteps	$21 \cdot 2^{-6j}$							

What are the possible downsides?

The Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_k$ be pairwise co-prime, and let $a_1, a_2, \ldots, a_k$ be any integers. Then the following system has a solution:

$$\begin{aligned} x &= a_1 \mod m_1 \\ x &= a_2 \mod m_2 \\ &\vdots \\ x &= a_k \mod m_k \end{aligned}$$

Further, any two solutions are congruent mod $m_1 m_2 \cdots m_k$

Example: Find all solutions to the system

$$x = 3 \mod 4$$

$$x = 2 \mod 5$$

$$x = 7 \mod 9$$