Birthday Attack for DLP ($g^x \equiv h \pmod p$)

List 1: g^k (random k)

List 2: hg^ℓ (random ℓ)

Runtime ?

Seek a collision: $g^k \equiv hg^\ell \pmod p$.

Example. $p = 113$, $g = 3$, $h = 34$

$g^k \equiv 2 \equiv hg^\ell$ when $k = 12$, $\ell = 5$

$g^k \equiv g^{x+\ell} \pmod{113}$

$k \equiv x + \ell \pmod{112}$

$x \equiv k - \ell \equiv 12 + 5 \equiv 17$.

Q: How long do the lists need to be?

Q: What is the probability of a collision with lists of a given length?

"Birthday Paradox"

n = # of people

Y = # of days in a year

Q: Prob. of collision?

$$\text{Prob(no collision)} = \underbrace{1}_{\text{1st person}} \cdot \underbrace{\left(1-\frac{1}{Y}\right)}_{\text{2nd}} \cdot \underbrace{\left(1-\frac{2}{Y}\right)}_{\text{3rd}} \cdot \left(1-\frac{3}{Y}\right) \cdots \underbrace{\left(1-\frac{n-1}{Y}\right)}_{n^{th}}$$

$$\underset{\text{approx.}}{\approx} e^{-n^2/2Y}$$

$$\text{Prob(a collision)} = 1 - e^{-n^2/2Y}$$

(good approx when n is mod. large)

2 Lists Version (DLP alg.): $\text{Prob(a collision)} = 1 - e^{-n^2/Y}$.

$$\text{Prob}(\text{collision}) \approx 1 - e^{-n^2/Y}$$

Corollary Two lists of length $n = \sqrt{Y}$ have a good prob. of a collision:

$$n \approx \sqrt{Y} \text{ gives } 1 - e^{-1} \approx 0.63.$$

Runtime: $O(\sqrt{p})$.

Baby-Step, Giant-Step Attack on DLP ($g^x \equiv h \pmod p$)

Runtime $O(\sqrt{p})$

0. Choose N s.t. $N^2 > p$.
1. Make list
$$g^k \quad 0 \le k \le N$$
2. Make list
$$hg^{-Nl} \quad 0 \le l \le N$$
3. Look for a match:
$$g^k \equiv hg^{-Nl} \pmod p$$
$$\Rightarrow h \equiv g^{k+Nl} \pmod p$$
$$\Rightarrow x \equiv k + Nl \pmod{p-1}.$$

Why does this work?

l \ k	0	1	2	3	...	$N-1$
0	0	1	2	3	...	$N-1$
1	N	$N+1$	...			
2						
⋮						
$N-1$						N^2-1

(Top-left cell: $k+Nl$)

Every $0 \le x \le p-1$ can be written uniquely as $x = k + Nl$ for $0 \le k, l < N$.

Index Calculus (to solve DLP $g^x \equiv h \pmod{p}$)

"Factor Base" = list of small primes up to some bound

$$p_1, \ldots, p_m \leq B$$

① Collect Data.

Compute $g^k \pmod{p}$ for random k's. (many)

Try to write the residue as $\prod_{i=1}^{m} p_i^{a_i}$.

Data: facts (Get many such facts)

$$g^k \equiv \prod_{i=1}^{m} p_i^{a_{i,k}} \pmod{p}.$$

② Transfer the data to exponents:

$$p_i = g^{L_g(p_i)}$$

facts (linear equations)

$$k \equiv \sum_{i=1}^{m} a_i \underbrace{L_g(p_i)}_{X_i} \pmod{p-1}$$

③ Solve the system of linear equations in unknowns X_i.

④ Use h

Write

$$h g^k \equiv \prod_{i=1}^{m} p_i^{a_i} \pmod{p}$$

(try random k until this works)

$$\Rightarrow x + k \equiv \sum_{i=1}^{m} a_i L_g(p_i) \pmod{p-1}$$

Solve for x.

Facts

$$g^9 \equiv 5^3 \pmod{p}$$

$$g^9 \equiv (g^x)^3 \pmod{p}$$

linear equations

$$9 \equiv 3x \pmod{p-1}$$

solve for x

$$x \equiv 3$$

$5 = g^x$ unknown x

$x = Lg(5)$