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.

$p = 127, \quad g = 3, \quad h = 71$

we should know!

Pick Factor Base: 2, 3

$2X \equiv 0 \pmod 6$ (0, 3)

$X \equiv 0 \pmod 6$

$2X \equiv 1 \pmod 5$

$2X \equiv 6 \pmod 5$

$X \equiv 3$

$X_2 = Lg(2)$

$X_3 = Lg(3)$

$g^{37} = 2^4 \cdot 3 \Rightarrow 37 \equiv 4X_2 + X_3 \pmod{126}$

$37 \equiv 4X_2 + 1$

$g^{74} = 2 \cdot 3^2 \Rightarrow 74 \equiv X_2 + 2X_3$

$g^{72} = 2 \cdot 3 \Rightarrow 73 \equiv X_2 + X_3$

$1 \equiv X_3$

$X_2 \equiv 72$

$h g^2 = 2^2$

$x + 2 \equiv 2X_2 \pmod{126}$

$x \equiv 2(72) - 2 \pmod{126}$

$\equiv 142$

Index Calculus Runtime (modulus size n)

$e^{\ln(\ln n)} = \ln n$

Very roughly $e^{(\ln n)^{1/2}} = e^{\sqrt{\ln n}} < e^{\ln n} < n$

"Sub-exponential"

The bottleneck is computing the factorizations (to get "facts") → factors in terms of primes $< B$.

Size of B: need g^k to be likely to be "B-smooth"

Fact: Prob of a $\# < X$ being $X^{1/u}$-smooth is approx $\frac{1}{u^u}$.

need high probability (large B)

and need low cost to test if factor (small B)

$\Rightarrow$ Balance

El Gamal : Encryption based on DLP.

Setup: $\mathbb{Z}/p\mathbb{Z}$, g = primitive root.

Alice

has a message
$0 \le m < p$
gets h

Bob

choose an random integer a
compute $h = g^a$

Public Key : h
Private Key : a

h ←

Encryption:
Choose secret integer k randomly
compute $r = g^k$
$t = h^k m$

g^{ak}

"ephemeral key pair"
k = private
r = public

(r, t) →

(r, t)

Decrypt:
$$\begin{aligned} & tr^{-a} \\ &= h^k m (g^k)^{-a} \\ &= g^{ak} m g^{-ak} \\ &= m \end{aligned}$$

Eve's Challenge

Given: p, g, h, r, t
Find: m

$\frac{1}{x} = x^{-1}$
$= x^{\varphi(n)-1}$

Thm. Breaking El Gamal is equivalent to the Computation Diffie-Hellman Problem. (CDHP)

Rephrase: Suppose E is an algorithm that breaks **El Gamal**
(Given $p, g, h = g^a, r = g^k, t = h^k m$, obtain m).

Suppose D " " " " **CDHP**
(Given p, g^x, g^y, obtain g^{xy}).

Then { E can be used to solve CDHP
{ D " " " El Gamal. (in polynomial time)

Pf. ① If we have E, and are given g^x, g^y then
input $(p, g, h, r, t) = (p, g, g^x, g^y, t)$ for any t
Then E output $m = t r^{-x} = t g^{-xy}$
Compute $t m^{-1} = g^{xy}$.

② If we have D and ciphertext (p, g, h, r, t)
then input $(h = g^a, r = g^k)$ to D. Get g^{ak}. Compute $m = t r^{-a} = t (g^{ak})^{-1}$ ☐