Splitting secret algorithm:

(a) Take a large prime p.

(b) Compute random $a_0, a_1, \dots, a_{k-1} \in \{0, 1, \dots, p-1\}$
$f(x) = a_{k-1} x^{k-1} + \dots + a_1 x + a_0$

(c) Tell person i the value $f(i) \pmod p$.

k people can combine their values and use LIF to derive $f(x)$.

$k-1$ people can not derive anything. In fact, for arbitrary $a_0 = f(0)$, valid polynomial $f(x)$ can be constructed.

§19 Algorithms for discrete log problem.

Recall; DLP: given prime p, $a, b \in \{1, 2, \dots, p-1\}$ such that $b^x \equiv a \pmod p$ for some x, find minimal such x ($\log_{b,p}(a)$).

Note: The general solution of $b^x \equiv a \pmod p$ is $x \equiv \log_{b,p}(a) \pmod N$ where $N = \mathrm{ord}_p(b)$.

No known polynomial time algorithms for DLP $\longrightarrow$ security of Diffie-Hellman, Elgamal.

Fastest known algorithm is Number Field Sieve, can do DLP for numbers p up to 160-200 digits.

Note: We assume that $N = \mathrm{ord}_p(b)$ is known. (computing N may be difficult in some cases).

§19.1 Naive approach.

Compute $b^0, b^1, b^2, b^3, \dots \pmod p$ until we find a.

It requires up to $N-1$ multiplications.

Example: $3^x \equiv 7 \pmod{31}$, $N = 30$.

$3^0 \equiv 1,\ 3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 27,\ 3^4 \equiv 19,\ 3^5 \equiv 26 \pmod{31}, \dots$

Trick to reduse the number of steps in halfi compute $a^{-1} \pmod p$. Then if $b^x \equiv a^{-1} \pmod p$ then $a \equiv b^{N-x} \pmod p$.

$7^{-1} \equiv 9 \pmod{31}$

$\Rightarrow 7^{-1} \equiv 3^2 \pmod{31} \Rightarrow 7 \equiv 3^{30-2} = 3^{28} \pmod{31}$

$x = 28$.

In total the complexity is $O(N)$ of multiplication mod p.

§19.2 Baby-step/Giant-step algorithm.

Let $M = \lceil \sqrt{N} \rceil$

We can write $x = My + z$ where $y, z \in \{0, 1, \dots, M-1\}$.

$$b^x \equiv a \pmod p \iff b^{My+z} \equiv a \pmod p$$

$$\iff b^z \equiv (b^{-M})^y \cdot a \pmod p.$$

Baby-step/Giant-step algorithm:

(a) Compute $b^0, b^1, b^2, \dots, b^{M-1} \pmod p$ and store them in memory.

(b) Compute $b^{-M} \pmod p$

(c) Compute $(b^{-M})^0 \cdot a, (b^{-M})^1 \cdot a, \dots \pmod p$ untill we find the coincidence with the first list.

Example: $2^x \equiv 65 \pmod{83}$. $N = 82$

$M = 10$.

(a)

i	0	1	2	3	4	5	6	7	8	9
$2^i \pmod{83}$	1	2	4	8	16	32	64	45	7	14

(b) $2^{10} \equiv 28 \pmod{83}$, $2^{-10} \equiv 3 \pmod{83}$

(c) $(2^{-10})^0 \cdot 65 \equiv 65 \pmod{83}$

$(2^{-10})^1 \cdot 65 \equiv 3 \cdot 65 \equiv 29 \pmod{83}$

$(2^{-10})^2 \cdot 65 \equiv 3 \cdot 29 \equiv 4 \pmod{83}$

We get $(2^{-10})^2 \cdot 65 \equiv 2^2 \pmod{83}$

$65 \equiv 2^{20+2} \equiv 2^{22} \pmod{83}$

$x = 22.$

Complexity: up to $\underset{\substack{\uparrow \\ \text{step (a)}}}{M-1} + \underset{\substack{\uparrow \\ \text{step (b)}}}{2} + \underset{\substack{\uparrow \\ \text{step (c)}}}{M-1} = 2M$

$= O(\sqrt{N})$ operations mod p.

§19.3 Pohling-Hellman algorithm.

Assume the factorization of N is

$$N = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}, \quad q_i \text{ are prime.}$$

Idea: compute x modulo $q_1^{\alpha_1}, q_2^{\alpha_2}, \ldots, q_r^{\alpha_r}$ and then use the CRT.

Let $d \mid N$.

Raise both parts in $b^x \equiv a \pmod{p}$ by power $\frac{N}{d}$

$$\left(b^{\frac{N}{d}}\right)^x \equiv a^{\frac{N}{d}} \pmod{p}$$

$\operatorname{ord}_p\left(b^{\frac{N}{d}}\right)$ is d.

$\left(\left(b^{\frac{N}{d}}\right)^d \equiv b^N \equiv 1 \pmod{p} \right.$

$\left. \text{For } j < d \quad \left(b^{\frac{N}{d}}\right)^j \equiv b^{\frac{Nj}{d}} \not\equiv 1 \pmod{p} \right)$

By solving $(b^{\frac{N}{d}})^x \equiv a^{\frac{N}{d}} \pmod{p}$

we find $x \equiv \log_{b^{\frac{N}{d}}, p}(a^{\frac{N}{d}}) \pmod{d}$.

Naive approach here will require ~~ok~~ up to d steps.

Example: $3^x \equiv 26 \pmod{127}$

$N = 126 = 2 \cdot 3^2 \cdot 7$.

Need to compute $x \pmod{2}$, $x \pmod{9}$, $x \pmod{7}$

(a) $x \pmod{2}$. $d=2$.

Raise equation to the power $\frac{126}{2} = 63$.

$3^{63} \equiv -1 \pmod{127}$, $26^{63} \equiv 1 \pmod{127}$.

$(-1)^x \equiv 1 \pmod{127} \implies x \equiv 0 \pmod{2}$.