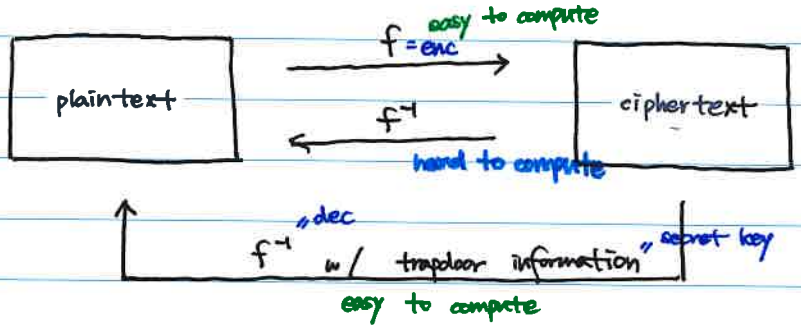
Chapter 2.2. The Discrete Logarithm Problem



- Structure; Let p be a prime.

  Then, for any $g \in \mathbb{Z}_p^*$, $\gcd(g, p) = 1$.

  By Fermat's Little Thm, $g^{p-1} \equiv 1 \mod p$.

  Moreover, $p-1$ is the smallest integer satisfying $g^x \equiv 1 \mod p$.

  By Thm, every nonzero element of $\mathbb{F}_p$ is equal to some power of (g).

  primitive root for $\mathbb{F}_p$

  $\therefore \mathbb{F}_p^* = \{1, g, g^2, \cdots, g^{p-2}\}$

Def. Let $g, h \in \mathbb{F}_p$.

Then, DLP is the problem of finding an exponent x s.t. $g^x \equiv h \mod p$.

A solving algorithm for DLP

- Naive (brute force): $O(2^n)$ where n is the bit size of p.
- BSGS : $O(2^{\sqrt{n}})$

  Let $x = im + j$ with $m = \lceil \sqrt{n} \rceil$. $0 \le i, j < m$.

  Then, $h \cdot (g^{-m})^i = g^j$ and pre-compute g^j for all j.