DTTF/NB479: Dszquphsbqiz Day 24

- Announcements:
  1. Term project groups and topics due midnight
  2. HW6 due next Tuesday.
- Questions?
- This week:
  - Primality testing, factoring
  - Discrete Logs, Computing Discrete Logs

Discrete logs…

But first, some humor:

Bruce Schneier is a genius in the crypto field, the author of the authoritative book on crypto.

Bruce Schneier writes his books and essays by generating random alphanumeric text of an appropriate length and then decrypting it.

Discrete logs…

….are the basis of the ElGamal cryptosystem

…can be used for digital signatures

Discrete Logs

Given $\beta = \alpha^x \pmod{p}$

Find x

We denote this as $x = L_\alpha(\beta)$

Why is this hard?

Consider this…

- Solve $9=2^x \pmod{11}$
- We denote the answer as $L_2(9)$

- Are there other solutions for x?

- By convention, x is defined to be the minimum of all such.
- It must be < (p-1). Why?

But consider this…

- Solve $2150=3621^x \pmod p$ where p=1775754…74581 (100 digits)
- How long will exhaustive search take?
  - Up to p-2 if 3621 is a *primitive root* of n.
- What's a primitive root?
- Please read section 3.7 (1 page) tonight if you haven't

One-way functions

- Take y=f(x)
- If y is easy to find given x, but x is hard to find given y, f is called a *one-way* function.
- Examples:
  - Factoring (easy to multiply, hard to factor)
  - Discrete logs (easy to find powers mod n, even if n is large, but hard to find discrete log)

Factoring vs. Discrete Logs

- Sizes of primes required are roughly similar
- We will encounter a number of discrete log algorithms that are analogs to factoring algorithms:
- (p-1) algorithm→Pollig-Hellman
- Quadratic sieve → Index calculus
- RSA → ElGamal

Finding x in $\beta \equiv \alpha^x$ is hard, but finding x (mod 2) isn't.

Assume α is a primitive root (mod p). So p-1 is the smallest *n* such that $\alpha^n \equiv 1$

By Fermat, $\left(\alpha^{\frac{p-1}{2}}\right)^2 \equiv \alpha^{p-1} \equiv 1(mod\ p)$

So $\alpha^{\frac{p-1}{2}} \equiv -1(mod\ p)$ (Can't be 1 since prim root)

To solve $\beta \equiv \alpha^x(mod\ p)$,

$$\beta^{\frac{p-1}{2}} \equiv \left(\alpha^{\frac{p-1}{2}}\right)^x \equiv (-1)^x\ (mod\ p)$$

$\left(\beta^{\frac{p-1}{2}}\right)^2 \equiv -1\ (mod\ p)$ iff $x \equiv 0\ (mod\ 2)$

Pollig-Hellman (section 7.2)

- Useful to solve $\beta \equiv \alpha^x (mod\ p)$ when *(p-1)* has only small prime factors
- Let $p - 1 = \prod_i q_i^{r_i}$
- Find x mod each q^r and combine using the Chinese Remainder Theorem
- Each one involves solving a discrete log problem, but over a very small domain: $0..q_i-1$.

- HW problem:

  solve $2^x=12 (\text{mod } 19)$ using Pollig-Hellman