CS 120/ E-177: Introduction to Cryptography

Salil Vadhan and Alon Rosen Oct. 17, 2006

Lecture Notes 8:

Computational Number Theory

Recommended Reading.

- Katz-Lindell 7, 8.1, 8.2, 8.4, 8.5

1 Sampling a Random Prime

Fact 1 (Prime Number Theorem) $\#\{primes \leq x\} \sim \frac{x}{\ln x}$ *as* $x \to \infty$*.*

How do we sample a random n-bit prime number in time $\text{poly}(n)$?

2 Modular arithmetic: $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$

Basic definitions:

- $x \equiv y \pmod{N}$ if $N | (x - y)$.
- $x \bmod N \stackrel{\text{def}}{=} [\text{unique } x' \in \{0, \ldots, N-1\} \text{ s.t. } x \equiv x' \pmod{N}]$.
- $\mathbb{Z}_N \stackrel{\text{def}}{=} \{0, \ldots, N-1\}$ with arithmetic $(+, \cdot)$ modulo N.

Fact 2 (Extended Euclidean Algorithm) *For any* $x, y \in \mathbb{N}$ *there exists two integers* a*,* b *such that* $ax + by = \gcd(x, y)$*. Moreover, such* a *and* b *can be found in polynomial time.*

Definition of $\mathbb{Z}_N^*$

$$\mathbb{Z}_N^* \stackrel{\text{def}}{=} \{x \in \mathbb{Z}_N : \gcd(x,N)=1\} = \text{elements of } \mathbb{Z}_N \text{ with multiplicative inverses}$$

By a multiplicative inverse for x we mean an element $y \in \mathbb{Z}_N$, denoted $y = x^{-1}$, such that $x \cdot y \equiv 1 \pmod{N}$. (the equality is proved using the Extended Euclidean Algorithm). Given N and $x \in \mathbb{Z}_N$, we can compute x^{-1} in polynomial time.

Euler phi function

$$\phi(N) \stackrel{\text{def}}{=} |Z_N^*|$$

Fact 3

$$\phi(N) = N \cdot \prod_{primes\ p|N} \left(1 - \frac{1}{p}\right) \geq \frac{N}{6\text{loglog}N}$$

This lower bound means that we can generate random elements from $\mathbb{Z}_N^*$ in time $\text{poly}(|N|) = \text{poly}(n)$: we pick a random element in $\mathbb{Z}_N$ and compute its gcd with N. If the gcd is equal to 1 then we have found an element of $\mathbb{Z}_N^*$. The probability of success is $\frac{\phi(N)}{N}$ so the expected number of trials is $\Theta\left(\frac{N}{\phi(N)}\right) = O(\text{loglog}N) = O(\log ||N||)$.
Computing $\phi(N)$ from N is as hard as factoring.

Groups

- A group G is a set G with binary operation $\star$ satisfying associativity, identity, inverses. All ours will also be commutative.
- Examples: $\mathbb{Z}_N$ under addition, $\mathbb{Z}_N^*$ under multiplication.
- Fact: In any group G, $\underbrace{x \star x \star \cdots \star x}_{|G|} = \text{id}$ for all $x \in G$.

  Corollary : $\forall x \in \mathbb{Z}_N^*,\ x^{\phi(N)} \equiv 1 \pmod{N}$

Facts about $\mathbb{Z}_p$ when p prime

- $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ (because $\phi(p) = p-1$) and $\mathbb{Z}_p$ is a *field*.
- **Fermat's Little Theorem:** For every $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$.
- A polynomial of degree d has at most d solutions mod p.
- For every prime p, there is a $g \in \mathbb{Z}_p^*$ such that $\{1 \bmod p, g \bmod p, g^2 \bmod p, g^3 \bmod p, \ldots, g^{p-2} \bmod p\} = \mathbb{Z}_p^*$. Such a g is called a *generator* of $\mathbb{Z}_p^*$.
- Discrete logarithm: For $x \in \mathbb{Z}_p^*$, $\log_g x \stackrel{\text{def}}{=} [\text{unique } i \in \{0,\ldots,p-2\} \text{ s.t. } g^i \equiv x \pmod{p}]$. Computing the discrete logarithm is believed to be hard, even if p and g are known.
- **Fact 4** *We can generate random n-bit prime p together with a (random) generator of $\mathbb{Z}_p^*$ time* $\text{poly}(n)$.

3 Chinese Remainder Theorem

Fact 5 (Chinese Remainder Theorem) *Let $N = pq$ with $\gcd(p, q) = 1$. Then the map $x \mapsto (x \mod p, x \mod q)$ from $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ is one-to-one and onto. In particular, for every $(y, z) \in \mathbb{Z}_p \times \mathbb{Z}_q$, there exists a unique $x \in \mathbb{Z}_N$ s.t. $x \equiv y \pmod{p}$ and $x \equiv z \pmod{q}$. Moreover, x can be found in polynomial time given (y, z, p, q).*

Proof: We will describe the inverse. By Extended Euclidean algorithm, can find a, b such that $ap+bq = gcd(p, q) = 1$. Let $c = bq$, $d = ap$ (*Chinese Remainder Coefficients*). Then $c \equiv 1 \pmod{p}$, $c \equiv 0 \pmod{q}$, $d \equiv 1 \pmod{q}$ and $d \equiv 0 \pmod{p}$. The inverse map is $(y, z) \mapsto x = cy + dz \mod N$.
We have

$$cy + dz \equiv 1 \cdot y + 0 \cdot z \equiv y \pmod{p}$$

and

$$cy + dz \equiv 0 \cdot y + 1 \cdot z \equiv z \pmod{q}$$

.
This shows that the map is onto and $|\mathbb{Z}_N| = |\mathbb{Z}_p \times Z_q|$ so the map is also one-to-one. The computation of x can be done in polynomial time because the extended Euclidean algorithm is $\text{poly}(||p||, ||q||)$ and we can compute c and d efficiently. ■

Using the Chinese Remainder Theorem, an arithmetic question modulo N can be reduced to an arithmetic problem modulo p and modulo q, *provided we know the factorization of N.*

4 Quadratic Residues

We define $\text{QR}_N \overset{\text{def}}{=} \{x^2 \bmod N : x \in \mathbb{Z}_N^*\}$.

Proposition 6 *When p odd prime, $|\text{QR}_p| = |\mathbb{Z}_p^*|/2 = (p-1)/2$.*

Proof: Consider the map from $\mathbb{Z}_p^* \to \mathbb{Z}_p^*$, given by $x \mapsto x^2$. A square in $\mathbb{Z}_p^*$ has at least two square roots because $a^2 \equiv (-a)^2 \mod p$ and $a \not\equiv -a \mod p$ as p is odd. A square in $\mathbb{Z}_p^*$ has at most two square roots: $\mathbb{Z}_p$ is a field so a polynomial of degree d has at most d roots modulo p. We consider the polynomial $x^2 - c \equiv 0 \pmod{p}$: for any c, the polynomial has at most two roots in $\mathbb{Z}_p$. The map is hence exactly 2 to 1. ■

Proposition 7 *When $N = pq$ for odd primes p, q, $|\text{QR}_N| = |\mathbb{Z}_N^*|/4$ and $x \mapsto x^2$ is 4-to-1 on $\mathbb{Z}_N^*$.*

Proof: Let us prove that $y \in \text{QR}_N \iff (y \mod p \in \text{QR}_p)$ and $(y \mod q \in \text{QR}_q)$.

Thus, by the Chinese Remainder Theorem $y \equiv (cx + dz)^2 \mod N$. The map $x \mapsto x^2$ is 4-to-1 on $\mathbb{Z}_N^*$.

$$|\text{QR}_N| = |\mathbb{Z}_N^*|/4 = \frac{(p-1)}{2} \cdot \frac{(q-1)}{2}$$

■