CS 346 Class Notes

Mark Lindberg

Apr 13, 2016

This Time:

Exam be done.

Prime order subgroup of $\mathbb{Z}_p^*$ (p prime).

$p = rq + 1$. p, q prime. Order q subgroup of $\mathbb{Z}_p^*$. $\{h^r \mod p \mid h \in \mathbb{Z}_p^*\}$. These are called the rth residuals modulo p.

It's very easy to show that this is a subgroup.

It is a bit more challenging to prove that the subgroup is order q.

Note that $p - 1 = rq$.

Idea of proof: Show that $f(h) = h^r \mod p$ is "r-to-1".

We need to show that groups of r elements each map to 1 element in our new group.

A result from last time, which now becomes useful: Proposition 8.53. Let G be a finite group, $g \in G$ an element of order i. Then $g^x = g^y \Leftrightarrow x \equiv y \pmod{()}i$.

Corollary: If g is a generator, $g^x = g^y \Leftrightarrow x \equiv y \pmod{|G|}$.

Back to the proof: Let g be a generator of $\mathbb{Z}_p^*$. Therefore, g has order $p - 1$ by theorem 8.56. The $g^0, g^1, \ldots, g^{p-2}$ are all of the elements of $\mathbb{Z}_p^*$.

Let $i, j \in \mathbb{Z}_{p-1}$.

Claim 1: g^i and g^j have the same rth residue mod p if and only if $q \mid (i - j)$.

Proof: Corollary above implies that $g^{ri} \equiv g^{rj}$, working in $\mathbb{Z}_p^*$, if and only if $ri \equiv rj \pmod{p-1}$ if and only if $r(i - j)$ is a multiple of $p - 1 = qr$, if and only if $i - j$ is a multiple of q.

Claim 2: $(g^0)^r, (g^1)^r, \ldots, (g^{q-1})^r$ are distinct.

Proof: Immediate from previous claim.

Claim 3: Let $\ell \in \mathbb{Z}_q$.

Then $g^\ell, g^{\ell+q}$, $g^{\ell+2q}, \ldots, g^{\ell+(r-1)q}$ all have the same rth residual modulo p.

Proof: Immediate from claim 1.

Advantages of this type of group G, the prime order subgroup:

1. We can generate a uniform random element of G: Choose h in $\mathbb{Z}_p^*$ uniformly at random. Take $h^r \mod p$.

2. We can identify a generator for G efficiently: Repeat 1) until we get an element $\neq$ identity.

3. We can efficiently test whether $h \in \mathbb{Z}_p^*$ belongs to G. Claim: $h \in G \Leftrightarrow h^g = 1$.

Proof of 3): Let $h = g^i$ where g is a generator of $\mathbb{Z}_p^*$. $i \in \mathbb{Z}_{p-1}$.
Claim 1: $h \in G \Leftrightarrow r \mid i$.
Proof: (IF) Assume $r \mid i$. Then $i = cr$, $h = g^{c^r} \Rightarrow h \in G$.
(ONLY IF) Assume $h \in G$. Then $h = (g^j)^r = g^{j^r}$ for some $j \in \mathbb{Z}_{p-1}$. By the corollary from the beginning of class, $i \equiv jr \pmod{p-1}$. Thus, $qr \mid (i - jr) \Rightarrow r \mid (i - jr) \Rightarrow r \mid i$.
Claim 2: $h^q = 1 \iff r \mid i$.

$$\begin{aligned} & h^q = 1 \\ \iff & g^{qi} = 1 = j^0 \\ \iff & (p-1) \mid qi \\ \iff & rq \mid qi \\ \iff & r \mid i \end{aligned}$$

"Discrete Log" Problem.
New experiment. $\mathsf{DLog}_{\mathcal{A},G}(n)$. We have G as a group generation algorithm. It generates $(\mathbb{G}, q, g)$, where $\mathbb{G}$ is a cyclic group of order q, and g is a generator of $\mathbb{G}$. Our security parameter is $||q|| = n$, the number of bits in the binary representation of q.
$\mathsf{DLog}_{\mathcal{A},G}(n)$:

- Run $G(1^n)$ to get $(\mathbb{G}, q, g)$.
- Pick h uniformly at random from G.
- $\mathcal{A}$ is given G, q, g, h, $\mathcal{A}$ outputs x.
- $\mathcal{A}$ succeeds if and only if $g^x = h$.

Definition 8.6.7: Discrete log is hard relative to G if $\forall$ PPT $\mathcal{A}$, $\Pr[\mathsf{DLog}_{\mathcal{A},G}(n) = 1] \leq \mathtt{negl}(n)$.
"Discrete log problem is hard" $\exists G$...
Section 8.4.2: Construction collision resistant hash functions given that we assume the discrete log problem is hard.
Construction 8.78. That's a lot of numbers. There is an explanation of this in the text. (I tend to space out at the end of classes, sorry. 2 classes in a row does that to me.)
Claim: Construction 8.78 gives a collision resistant hash function assuming the discrete-log problem is hard relative to G.
Idea of proof: Show that a collision enables us to compute the discrete log of h.