Bits and Pieces of Ch 8

Wednesday, November 1, 2023 10:35 AM

§ 8.3 Cryptographic Assumptions in Cyclic Groups

Story:

- In this section
  we introduce a class of cryptographic hardness assumptions in *cyclic groups.*
  - We begin with a general discussion of cyclic groups
    followed by abstract definitinos of the relevant assumptions.
  - We then look at two concrete and widel used
    examples of cyclic groups in which
    these assumptions are believed to hold.

§ 8.3.1 Cyclic Groups and Generators

Let G be a finite group of order m.

For arbitrary $g \in G$, consider the set

$\langle g \rangle \coloneqq \{g^0, g^1 \dots\}$.

(Warning: If G is an infinite group, $\langle g \rangle$ is defined differently)

(NB for me: $\langle g \rangle \neq G$ in general; it is just a subgroup)

By Theorem 8.14
we have $g^m = 1$.

Let $i \leq m$ be the smallest positive integer
for which $g^i = 1$.

Then, the above sequence
repeats after i terms
(i.e. $g^i = g^0$, $g^{i+1} = g^1$ etc.)

and so

$\langle g \rangle = \{g^0, \dots g^{i-1}\}$.

Observe that $\langle g \rangle$ contains at most i elements.

In fact, it contains exactly i elements
(otherwise i is not the smallest integer for which $g^i = 1$).

It is not hard to verify that $\langle g \rangle$ is a subgroup of G for any g
(see Exercise 8.3).

We call $\langle g \rangle$ the *subgroup generated by g.*

If the order of the subgroup $\langle g \rangle$ is i
then i is called the *order of g*; i.e.

DEFINITION 8.51 *Let $\mathbb{G}$ be a finite group and $g \in \mathbb{G}$. The* order *of g is the smallest positive integer i with $g^i = 1$.*

The following is a useful analogue of Corollary 8.15

PROPOSITION 8.52 *Let $\mathbb{G}$ be a finite group, and $g \in \mathbb{G}$ an element of order i. Then for any integer x, we have $g^x = g^{[x \bmod i]}$.*

Rough
Suppose G is a finite group.

~~Claim: Take any $g \in G$.~~
~~Then $\langle g \rangle = G$.~~

~~$\forall g' \in G, \exists k$ s.t. $g^k = g' \in G$~~

~~not true: e.g. $g = 1$~~

$\boxed{\text{Claim: If } G \text{ has at most } i \text{ elements, then } g^{i+1} = g. \Rightarrow g^i = 1}$

Proof sketch:

g

$g^2 = g$ or $g^2 \neq g$

done

$g^3 = g$; $g^3 \neq g$ "?" $\Rightarrow$ $g^3 \neq g^2$

done

$g^4 = g$

done

Suppose $g^3 = g^2$

$\Rightarrow g^2 = g$
violates previous branch.

g · g · g · g^2 · g^2 · g^3

A different proof that $g^? = 1$ when G is Abelian

$g_1 \quad g_2 \dots \quad g_m$

$g_1 \cdot g_2 \cdot \dots \cdot g_m =$

claim
$= g_1 \cdot g \quad g_2 \cdot g \quad g_m \cdot g = g_1 g_2 \cdots g_m g^m$

true: multiplicative group

$= g \cdot g_2 \cdots g_m$

$= g_1 \cdot g \quad g_2 \cdot g \quad g_m \cdot g = g_1 g_2 \cdots g_m g^{\cdots}$

$= g \cdot g_2 \cdots g_m$

true ∵ multiplication by a group element is simply a permutation on the group.

PROPOSITION 8.52 *Let $\mathbb{G}$ be a finite group, and $g \in \mathbb{G}$ an element of order i. Then for any integer x, we have $g^x = g^{[x \bmod i]}$.*

Basically, $g^x = g^{r+ki} = g^r g^{ki} = g^r$ where $x = r + ki$
where r is the remainder $(x \backslash mod\ i)$

We can prove something stronger:

Proposition 8.53

Let G be a finite group and $g \in G$ an element of order i.

Then $g^x = g^y$ iff $x = y \bmod i$.

PROOF If $x = y \bmod i$ then $[x \bmod i] = [y \bmod i]$ and the previous proposition says that

$$g^x = g^{[x \bmod i]} = g^{[y \bmod i]} = g^y.$$

For the more interesting direction, say $g^x = g^y$. Then $1 = g^{x-y} = g^{[x-y \bmod i]}$ (using the previous proposition). Since $[x - y \bmod i] < i$, but i is the smallest positive integer with $g^i = 1$, we must have $[x - y \bmod i] = 0$. ■