Cryptography

Lecture 20

Announcements

- HW 7 due 4/26

Agenda

- Last time:
  - Number theory
  - Hard problems (Factoring, RSA)
- This time:
  - More number theory (cyclic groups)
  - Hard problems (Discrete log and Diffie-Hellman problems)
  - Elliptic Curve groups

Cyclic Groups

For a finite group G of order m and $g \in G$, consider:

1

$g^m = 1 = g^0$

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

$\langle g \rangle$ always forms a cyclic subgroup of G.

However, it is possible that there are repeats in the above list.

Thus $\langle g \rangle$ may be a subgroup of order smaller than m.

If $\langle g \rangle = G$, then we say that G is a cyclic group and that g is a generator of G.

Examples

Consider Z^*_{13}: order of $Z^*_{13} = \boxed{12}$

2 is a generator of Z^*_{13}:

2^0	1
2^1	2
2^2	4
2^3	8
2^4	$16 \to 3$
2^5	6
2^6	12
2^7	$24 \to 11$
2^8	$22 \to 9$
2^9	$18 \to 5$
2^{10}	10
2^{11}	$20 \to 7$
2^{12}	$14 \to 1$

$g^m \hookrightarrow$

3 is not a generator of Z^*_{13}:

3^0	1
3^1	3
3^2	9
3^3	$27 \to 1$
3^4	3
3^5	9
3^6	$27 \to 1$
3^7	3
3^8	9
3^9	$27 \to 1$
3^{10}	3
3^{11}	9
3^{12}	$27 \to 1$

3 $\quad 3 \mid 12$

$3^{8 \bmod 3} = 3^2$

Definitions and Theorems

Definition: Let G be a finite group and $g \in G$. The order of g is the smallest positive integer i such that $g^i = 1$. = the order of the Subgroup generated by g

Ex: Consider Z_{13}^*. The order of 2 is 12. The order of 3 is 3.

Proposition 1: Let G be a finite group and $g \in G$ an element of order i. Then for any integer x, we have $g^x = g^{x \bmod i}$.

Proposition 2: Let G be a finite group and $g \in G$ an element of order i. Then $g^x = g^y$ iff $x \equiv y \bmod i$.

Th: G finite group of order m, $g \in G$.

Let i be the order of g, then $i \mid m$.

Proof. $g^i = 1$ (since i is order of g)

$g^m = 1$ (by generalized theorem)

$\Rightarrow g^i = g^m \Rightarrow i \equiv m \bmod i$ by Prop 2.

$\Rightarrow i \mid (m-i)$ by def of modulo.

$\Rightarrow i \mid m$ (since $i \mid i$). $\boxed{\checkmark}$

More Theorems

Proposition 3: Let G be a finite group of order m and $g \in G$ an element of order i. Then $i \mid m$.

Proof:

- We know by the generalized theorem of last class that $g^m = 1 = g^0$.
- By Proposition 2, we have that $0 \equiv m \bmod i$
- By definition of modulus, this means that $i|m$.

Corollary: if ~~G is a group of prime order p,~~ then G is cyclic and all elements of G except the identity are generators of G.

Why does this follow from Proposition 3?

Theorem: If p is prime then Z^*_p is a cyclic group of order $p-1$.

There exists a generator $g \in Z^*_p$.

use this to construct prime order group

Prime-Order Cyclic Groups

Consider Z^*_p, where p is a strong prime.

- Strong prime: $p = 2q + 1$, where q is also prime.
- Recall that Z^*_p is a cyclic group of order $p - 1 = 2q$.

perfect squares.

The subgroup of quadratic residues in Z^*_p is a cyclic group of prime order q.

Example of Prime-Order Cyclic Group

Consider Z^*_{11}.

Note that 11 is a strong prime, since $11 = 2 \cdot 5 + 1$. prime-

$\boxed{g = 2}$ is a generator of Z^*_{11}:

2^0	1
2^1	2
2^2	4
2^3	8
2^4	$16 \to 5$
2^5	10
2^6	$20 \to 9$
2^7	$18 \to 7$
2^8	$14 \to 3$
2^9	6

The even powers of g are the "quadratic residues" (i.e. the perfect squares). Exactly half the elements of Z^*_p are quadratic residues.

Note that the even powers of g form a cyclic subgroup of order $\frac{p-1}{2} = q$.

$2^8 \cdot 2^6 = 2^{14 \bmod 10} = 2^4$ even number between 0 and $p-2$.

$p-1$ is even

Verify:

- closure (Multiplication translates into addition in the exponent. Addition of two even numbers mod $p-2$ gives an even number mod $p-1$, since for prime $p > 3$, $p-1$ is even.)
- Cyclic –any element is a generator. E.g. it is easy to see that all even powers of g can be generated by g^2.

The Discrete Logarithm Problem (DL)

The discrete-log experiment $DLog_{A,\boldsymbol{G}}(n)$

1. Run $\boldsymbol{G}(1^n)$ to obtain (G, q, g) where G is a cyclic group of order q (with $||q|| = n$) and g is a generator of G. number of bits in q.
2. Choose a uniform $h \in G$
3. A is given G, q, g, h and outputs $x \in Z_q$

   $\boxed{x = \log_g h}$

4. The output of the experiment is defined to be 1 if $g^x = h$ and 0 otherwise.

$\{g^0, g^1, g^x, g^{q-1}\}$ $\quad g^x = h$ $\quad x \in \mathbb{Z}_q$

Definition: We say that the DL problem is hard relative to $\boldsymbol{G}$ if for all ppt algorithms A there exists a negligible function neg such that

$$\Pr\left[DLog_{A,\boldsymbol{G}}(n) = 1\right] \leq neg(n).$$

The Diffie-Hellman Problems

Diffie-Hellman

The CDH Problem

Computational

Given (G, q, g) and uniform $h_1 = g^{x_1}, h_2 = g^{x_2}$, compute $g^{x_1 \cdot x_2}$.

$x_1 \xleftarrow{R} \mathbb{Z}_q$, $x_2 \xleftarrow{R} \mathbb{Z}_q$

Given: (G, q, g) $h_1 = g^{x_1}$, $h_2 = g^{x_2}$

Goal: Compute $g^{x_1 \cdot x_2} = (h_1)^{\mathrm{dlog}_g h_2} = (g^{x_1})^{x_2} = g^{x_1 \cdot x_2}$

Break DLog $\rightarrow$ Break CDH

?

The DDH Problem

We say that the DDH problem is hard relative to $\boldsymbol{G}$ if for all ppt algorithms A, there exists a negligible function neg such that

$$|\Pr[A(G,q,g,g^x,g^y,g^z)=1]$$
$$-\Pr[A(G,q,g,g^x,g^y,g^{xy})=1]| \leq neg(n).$$

Random Tuple World		DDH Tuple World
(g^x, g^y, g^z)	D	$(G,q,g)\ (g^x, g^y, g^{xy})$
$x,y,z \xleftarrow{R} \mathbb{Z}_q$		$x,y \xleftarrow{R} \mathbb{Z}_q$

DDH problem completely broken $\boxed{\mathbb{Z}_p^*}$, p strong prime

different group: subgroup of quadratic residues in $\mathbb{Z}_p^*$, p strong prime.

Breaking DDH $\not\to$ Breaking CDH.

CDH is believed hard in $\mathbb{Z}_p^*$, DDH is easy.

Why can you break DDH in $\mathbb{Z}_p^*$?

Legendre symbol an efficient way to check whether $h \in \mathbb{Z}_p^*$ is a quadratic residue.

$h = \ell^2$ for some $\ell \in \mathbb{Z}_p^*$. g is a generator of $\mathbb{Z}_p^*$

(g^x, g^y, g^z)

0	0	0	|	1	0	0
0	0	1	|	1	0	1

(g^x, g^y, g^{xy}).

0 0 0

(h_1, h_2, h_3)

h_1: quad res? h_2: QR? h_3: QR

0 1 0 | 1 1 0   1 0 1
0 1 1 | $\boxed{1\ 1\ 1}$ 0 1 1
$\boxed{1\ 1\ 1}$

Relative Hardness of the Assumptions

Breaking DLog → Breaking CDH → Breaking DDH

DDH Assumption → CDH Assumption → DLog Assumption