Cryptography

Lecture 21

Announcements

- HW 7 due today
- HW 8 up on course webpage, due 4/29

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:

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

$\langle g \rangle$ 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 $Z^*{}_{13}$:

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

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

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

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

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 $g^i = 1$.

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 $x \equiv y \bmod i$.

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 1, we have that $g^m = g^{m \bmod i} = g^0$.
- By the ← direction of Proposition 2, we have that $0 \equiv m \bmod i$.
- By definition of modulus, this means that $i \mid m$.

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 $p - 1$.

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 $p - 1 = 2q$.

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 $11 = 2 \cdot 5 + 1$.

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

2^0	1
2^1	2
2^2	4
2^3	8
2^4	$16 \rightarrow 5$
2^5	10
2^6	$20 \rightarrow 9$
2^7	$18 \rightarrow 7$
2^8	$14 \rightarrow 3$
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 $\frac{p-1}{2} = q$.

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

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.
2. Choose a uniform $h \in G$
3. A is given G, q, g, h and outputs $x \in Z_q$
4. The output of the experiment is defined to be 1 if $g^x = h$ and 0 otherwise.

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

The CDH Problem

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

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

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

Relative Hardness of the Assumptions

Breaking DLog → Breaking CDH → Breaking DDH

DDH Assumption → CDH Assumption → DLog Assumption

Elliptic Curves over Finite Fields

- Z_p is a finite field for prime p.
- Let $p \geq 5$ be a prime
- Consider equation E in variables x, y of the form:

$$y^2 := x^3 + Ax + B \; mod \; p$$

Where A, B are constants such that $4A^3 + 27B^2 \neq 0$.
(this ensures that $x^3 + Ax + B \; mod \; p$ has no repeated roots).
Let $E(Z_p)$ denote the set of pairs $(x, y) \in Z_p \times Z_p$ satisfying the above equation as well as a special value O.

$$E(Z_p) := \{(x, y) | x, y \in Z_p \; and \; y^2 = x^3 + Ax + B \; mod \; p\} \cup \{O\}$$

The elements $E(Z_p)$ are called the points on the Elliptic Curve E and O is called the point at infinity.

Elliptic Curves over Finite Fields

Example:

Quadratic Residues over Z_7.

$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9 = 2, 4^2 = 16 = 2, 5^2 = 25 = 4, 6^2 = 36 = 1.$

$f(x) \coloneqq x^3 + 3x + 3$ and curve $E: y^2 = f(x)\ mod\ 7$.

- Each value of x for which $f(x)$ is a non-zero quadratic residue mod 7 yields 2 points on the curve
- Values of x for which $f(x)$ is a non-quadratic residue are not on the curve.
- Values of x for which $f(x) \equiv 0\ mod\ 7$ give one point on the curve.

Elliptic Curves over Finite Fields

$f(0) \equiv 3 \, mod \, 7$	a quadratic non-residue mod 7
$f(1) \equiv 0 \, mod \, 7$	so we obtain the point $(1,0) \in E(Z_7)$
$f(2) \equiv 3 \, mod \, 7$	a quadratic non-residue mod 7
$f(3) \equiv 4 \, mod \, 7$	a quadratic residue with roots $2,5$. so we obtain the points $(3,2), (3,5) \in E(Z_7)$
$f(4) \equiv 2 \, mod \, 7$	a quadratic residue with roots $3,4$. so we obtain the points $(4,3), (4,4) \in E(Z_7)$
$f(5) \equiv 3 \, mod \, 7$	a quadratic non-residue mod 7
$f(6) \equiv 6 \, mod \, 7$	a quadratic non-residue mod 7