Introduction to Cryptology

Lecture 21

Announcements

- HW 8 due today
- HW 9 up on course webpage
  - Due on Tuesday, 5/1.

Agenda

- Last time:
  - Factoring
  - RSA
  - Cyclic Groups

- This time:
  - More on Cyclic Groups
  - Hard problems over cyclic groups
  - Elliptic Curve Groups

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 $\rightarrow$ Breaking CDH $\rightarrow$ Breaking DDH

DDH Assumption $\rightarrow$ CDH Assumption $\rightarrow$ DLog Assumption

Elliptic Curves over Finite Fields

Why use them?

- No known sub-exponential time algorithm for solving DL in appropriate Curves.
- Implementation will be more efficient.

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.