Introduction to Cryptology

Lecture 22

Announcements

- HW7 due today
- HW8 up on course webpage. Due Tuesday, 5/2.

Agenda

- Last time:
  - Groups Z_N^*, for general N
  - Cyclic Groups $\langle g \rangle$
- This time:
  - Cyclic Groups, prime order groups
  - Hard problems
  - Elliptic Curve Groups

Cyclic Groups

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

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

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

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 $g^x = g^{x \, mod \, i}$.

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

More Theorems

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

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 $\leftarrow$ direction of 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 $p - 1$.

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 Factoring Assumption

The factoring experiment $Factor_{A,Gen}(n)$:

1. Run $Gen(1^n)$ to obtain (N, p, q), where p, q are random primes of length n bits and $N = p \cdot q$.
2. A is given N, and outputs $p', q' > 1$.
3. The output of the experiment is defined to be 1 if $p' \cdot q' = N$, and 0 otherwise.

Definition: Factoring is hard relative to Gen if for all ppt algorithms A there exists a negligible function neg such that

$$\Pr[Factor_{A,Gen}(n) = 1] \leq neg(n).$$

How does Gen work?

1. Pick random n-bit numbers p, q
2. Check if they are prime
3. If yes, return (N, p, q). If not, go back to step 1.

Why does this work?

- Prime number theorem: Primes are dense!
  - A random n-bit number is a prime with non-negligible probability.
  - Bertrand's postulate: For any $n > 1$, the fraction of n-bit integers that are prime is at least $1/3n$.
- Can efficiently test whether a number is prime or composite:
  - If p is prime, then the Miller-Rabin test always outputs "prime." If p is composite, the algorithm outputs "composite" except with negligible probability.

The RSA Assumption

The RSA experiment $RSA - inv_{A,Gen}(n)$:

1. Run $Gen(1^n)$ to obtain (N, e, d), where $\gcd\big(e, \phi(N)\big) = 1$ and $e \cdot d \equiv 1 \: mod \: \phi(N)$.
2. Choose a uniform $y \in {Z^*}_N$.
3. A is given (N, e, y), and outputs $x \in {Z^*}_N$.
4. The output of the experiment is defined to be 1 if $x^e = y \: mod \: N$, and 0 otherwise.

Definition: The RSA problem is hard relative to Gen if for all ppt algorithms A there exists a negligible function neg such that

$$\Pr\big[RSA - inv_{A,Gen}(n) = 1\big] \leq neg(n).$$

Relationship between RSA and Factoring

Known:

- If an attacker can break factoring, then an attacker can break RSA.
  - Given p, q such that $p \cdot q = N$, can find $\phi(N)$ and d, the multiplicative inverse of $e \ mod \ \phi(N)$.
- If an attacker can find $\phi(N)$, can break factoring.
- If an attacker can find d such that $e \cdot d \equiv 1 \ mod \ \phi(N)$, can break factoring.

Not Known:

- Can every efficient attacker who breaks RSA also break factoring?

Due to the above, we have that the RSA assumption is a stronger assumption than the factoring assumption.