Cryptography

Lecture 18

Announcements

- HW 4 due 4/10 (only problems 1-7)

Agenda

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

Multiplicative Groups Mod N

- What about multiplicative groups modulo N, where N is composite?
- Which numbers $\{1, \ldots, N-1\}$ have multiplicative inverses $mod\ N$?
  - a such that $\gcd(a, N) = 1$ has multiplicative inverse by Extended Euclidean Algorithm.
  - a such that $\gcd(a, N) > 1$ does not, since $\gcd(a, N)$ is the smallest positive integer that can be written in the form $Xa + YN$ for integer X, Y.
- Define $Z_N^* := \{a \in \{1, \ldots, N-1\} \mid \gcd(a, N) = 1\}$.
- Z_N^* is an abelian, multiplicative group.
  - Why does closure hold?

Order of Multiplicative Groups Mod N

- What is the order of Z_N^*?
- This has a name. The order of Z_N^* is the quantity $\phi(N)$, where ϕ is known as the Euler totient function or Euler phi function.
- Assume $N = p \cdot q$, where p, q are distinct primes.
  - $\phi(N) = N - p - q + 1 = p \cdot q - p - 1 + 1 = (p-1)(q-1)$.
  - Why?

Order of Multiplicative Groups Mod N

General Formula:

Theorem: Let $N = \prod_i p_i^{e_i}$ where the $\{p_i\}$ are distinct primes and $e_i \geq 1$. Then

$$\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1).$$

Another Special Case of Generalized Theorem

Corollary of generalized theorem:

For a such that $\gcd(a, N) = 1$:

$$a^{\phi(N)} \equiv 1 \; mod \; N.$$

$\mathbb{Z}^*_N$

$|\mathbb{Z}^*_N| = \phi(N)$

$\equiv a^0 \; mod \; N$

base

$mod \; \phi(N)$

Another Useful Theorem

Theorem: Let G be a finite group with $m = |G| > 1$. Then for any $g \in G$ and any integer x, we have

$$g^x = g^{x \bmod m}.$$

b ≡ x mod m

$g^{m-1} = g^{-1}$ — inverse of g in G

Proof: We write $x = a \cdot m + b$, where a is an integer and $b \equiv x \bmod m$.

- $g^x = g^{a \cdot m + b} = (g^m)^a \cdot g^b$
- By "generalized theorem" we have that

$$(g^m)^a \cdot g^b = 1^a \cdot g^b = g^b = g^{x \bmod m}.$$

An Example:

$\mathbb{Z}_{35}^*$

Compute $3^{25} \; mod \; 35$ by hand.

$$\phi(35) = \phi(5 \cdot 7) = (5-1)(7-1) = 24$$

$$3^{25} \equiv 3^{25 \; mod \; 24} \; mod \; 35 \equiv 3^1 \; mod \; 35$$

$$\equiv 3 \; mod \; 35.$$

Modular Exponentiation

efficient alg's : polynomial in log(N) modulus.

Efficient	Hard Problems
1. group operation mod N	
2. finding inverses	
3. exponentiation?	

Modular Exponentiation

Is the following algorithm efficient (i.e. poly-time)?

$a \in \mathbb{Z}_N^*$

ModExp(a, m, N) //computes $a^m \, mod\, N$

Set $temp := 1$

For $i = 1$ to m

Set $temp := (temp \cdot a) mod\ N$

return $temp$;

Aside: Compute $3^{2^{128}}$ over the integers

just writing this down takes more than 2^{128} # of bits.

Modular Exponentiation

Is the following algorithm efficient (i.e. poly-time)?

ModExp(a, m, N) //computes $a^m \; mod \; N$

Set $temp := 1$

For $i = 1$ to m

Set $temp := (temp \cdot a) mod \; N$

return $temp$;

No—the run time is $O(m)$. m can be on the order of N.
This means that the runtime is on the order of $O(N)$,
while to be efficient it must be on the order of $O(\log N)$.

Modular Exponentiation

We can obtain an efficient algorithm via "repeated squaring."

ModExp(a, m, N) //computes $a^m \ mod \ N$, where $m = m_{n-1} m_{n-2} \cdots m_1 m_0$ are the bits of m.

Set $s := a$
Set $temp := 1$
For $i = 0$ to $n - 1$
  If $m_i = 1$
    Set $temp := (temp \cdot s) mod \ N$
  Set $s := s^2 \ mod \ N$ → repeated squaring
return $temp$;

This is clearly efficient since the loop runs for n iterations, where $n = \log_2 m$.

Modular Exponentiation

Why does it work?

$$m = \sum_{i=0}^{n-1} m_i \cdot 2^i$$

Consider $a^m = a^{\sum_{i=0}^{n-1} m_i \cdot 2^i} = \prod_{i=0}^{n-1} a^{m_i \cdot 2^i}$.

$s = a^{(2^i)}$
in the ith iteration

In the efficient algorithm:

s values are precomputations of a^{2^i}, for $i = 0 \; to \; n-1$ (this is the "repeated squaring" part since $a^{2^i} = (a^{2^{i-1}})^2$).

If $m_i = 1$, we multiply in the corresponding s-value.

If $m_i = 0$, then $a^{m_i \cdot 2^i} = a^0 = 1$ and so we skip the multiplication step.

Cyclic Groups

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

$g^s = 1$

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

$\langle g \rangle$ 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}	$27 \rightarrow 1$

$\mathbb{Z}^*_p$ p is prime is always a cyclic group

order of $\mathbb{Z}^*_p$, p is prime: $p-1$.

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 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 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