Introduction to Cryptology

Lecture 21

Announcements

- HW7 due Tuesday 4/25

Agenda

- Last time:
  - Repeated Squaring Algorithm
  - Extended Euclidean Algorithm
  - Chinese Remainder Theorem

- This time:
  - More Number theory background
  - Hard problems

Generalized Theorem

Theorem: Let G be a finite group with $m = |G|$, the order of the group. Then for any element $g \in G, g^m = 1$.

Corollary of Fermat's Little Theorem is a special case of the above when G is the multiplicative group ${Z^*}_p$ and p is prime.

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 $Z^*{}_N \coloneqq \{a \in \{1, \ldots, N-1\} |\gcd(a, N) = 1\}$.
- $Z^*{}_N$ 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 $\gcd(a, N) = 1$:

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

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

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

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:

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

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

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

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

Background for RSA

Recall that we saw last time that

$$a^m \equiv a^{m \bmod \phi(N)} \bmod N.$$

For $e \in {Z^*}_N$, let $f_e: Z_N^* \to Z_N^*$ be defined as $f_e(x) := x^e \bmod N$.

Theorem: $f_e(x)$ is a permutation.
Proof: To prove the theorem, we show that $f_e(x)$ is invertible.
Let d be the multiplicative inverse of $e \bmod \phi(N)$.
Then for $y \in Z_N^*$, $f_d(y) := y^d \bmod N$ is the inverse of f_e.

To see this, we show that $f_d(f_e(x)) = x$.
$f_d(f_e(x)) = (x^e)^d \bmod N = x^{e \cdot d} \bmod N = x^{e \cdot d \bmod \phi(N)} \bmod N = x^1 \bmod N = x \bmod N$.

Note: Given d, it is easy to compute the inverse of f_e
However, we saw in the homework that given only e, N, it is hard to find d, since finding d implies that we can factor $N = p \cdot q$.
This will be important for cryptographic applications.

Toolbox for Cryptographic Multiplicative Groups

Can be done efficiently	No efficient algorithm believed to exist
Modular multiplication	Factoring
Finding multiplicative inverses (extended Euclidean algorithm)	RSA problem
Modular exponentiation (via repeated squaring)	Discrete logarithm problem
	Diffie Hellman problems

We have seen the efficient algorithms in the left column.
We will now start talking about the “hard problems” in the right column.

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}	$27 \rightarrow 1$