Introduction to Cryptology

Lecture 20

Announcements

- HW8 due Tuesday, 4/19
- TA OH Monday 4/18 4pm-6pm

Agenda

- More Number Theory!

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 $\{1, \dots, N-1\}$ 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 ${Z^*}_N \coloneqq \{a \in \{1, \dots, N-1\} | \gcd(a, N) = 1\}$.
- ${Z^*}_N$ 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 $f_e(x) \coloneqq x^e \bmod N$.

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 $y \in Z^*_N$, $f_d(y) \coloneqq y^d \bmod N$ 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.

Chinese Remainder Theorem

Going from $(a, b) \in Z_p \times Z_q$ to $x \in Z_N$

Find the unique $x \; mod \; N$ such that

$$x \equiv a \; mod \; p$$
$$x \equiv b \; mod \; q$$

Recall since $\gcd(p, q) = 1$ we can write

$$Xp + Yq = 1$$

Note that

$$Xp \equiv 0 \; mod \; p$$
$$Xp \equiv 1 \; mod \; q$$

Whereas

$$Yq \equiv 1 \; mod \; p$$
$$Yq \equiv 0 \; mod \; p$$

Going from $(a, b) \in Z_p \times Z_q$ to $x \in Z_N$

Find the unique $x \; mod \; N$ such that

$$x \equiv a \; mod \; p$$
$$x \equiv b \; mod \; q$$

Claim:

$$b \cdot Xp + a \cdot Yq \equiv a \; mod \; p$$
$$b \cdot Xp + a \cdot Yq \equiv b \; mod \; q$$

Therefore, $x \equiv b \cdot Xp + a \cdot Yq \; mod \; N$