6.857 Recitation 6: Number Theory and Diffie Hellman

Heeyoon Kim

1 Administrivia

- Project proposal due Fri. 3/24
- Pset 3 due Mon. 3/27

2 Introduction

This recitation is a review of Monday's and Wednesday's lectures on number theory, cryptographic groups, and Diffie Hellman Key Exchange.

3 Huge Prime Number Generation

Fermat:

1. Generate random k-bit number, p.
2. Accept if passes Fermat Test. $2^p = 1 \mod p$. Can use repeated squaring for efficiency.
3. Else, repeat random generation and Fermat Test.

Works because prime numbers are dense, e.g. there are often enough prime numbers. However to get better accuracy, could use Miller Rabin Primality Test. You don't have to know the details of this.

4 Safe Primes and Sophie Germain Primes

If q is a prime, and $p = 2q + 1$ is also a prime, p is a safe prime, and q is a Sophie Germain prime.

Thm 1. *If $p = 2q + 1$ is a prime, $\forall a \in Z_p^*$, $order_p(a) \in \{1, 2, q, 2q\}$*

Finding generators are hard, but if p is a safe prime, finding $g \in Z_p^*$ is easy.

Algorithm:

1. Generate random $g \in Z_p^*$
2. Check that:

- $g^{2q} = 1 \mod p$
- $g^q \neq 1 \mod p$
- $g^2 \neq 1 \mod p$

5 Order of Element

Definition 1. *Order(a) = smallest $u > 0$ s.t. $a^u = 1$ in G*

Definition 2. *If $< a >= G$, then G is cyclic with generator a. $| < a > |$ = order(a)*

6 Cryptographic Groups

In cryptography, often consider groups of numbers modular n or p.

Definition 3. $Z_p^* = \{1, 2, ..., p-1\}$ = *numbers relatively prime to p, where p is prime.* $|Z_p^*| = p - 1$

Example: $Z_7^* = \{1, 2, 3, 4, 5, 6\}$
Often, a safe prime is chosen for p. Half of Z_p^* are generators, the other half are squares. Z_p^* is always cyclic.

Definition 4. $Z_n^* = \{a \in \{1, 2, ...n-1\} : gcd(a, n) = 1\}$ = *numbers relatively prime to n.*

Example: $Z_{10} = \{1, 3, 7, 9\}$

Definition 5. $|Z_n^*| = \phi(n)$

Example: $|Z_{52}^*| = \phi(n) = 52 \cdot \frac{1}{2} \cdot \frac{12}{13} = 24$

Thm 2. *(Euler's Thm).* $\forall a \in Z_n^*, a^{\phi(n)} = 1 \mod n$

Definition 6. Q_p = *quadratic residues* $= \{a^2 : a \in Z_p^*\}$

$|Q_p| = \frac{1}{2}|Z_p^*| = \frac{p-1}{2}$ ($= q$ if $p = 2q + 1$).
The size is halved because $a^2 \mod p$ and $(p-a)^2 = (-a)^2 \mod p$ would both map to $a^2 \mod p$

Definition 7. Q_n = *quadratic residues mod n* $= \{a^2 : a \in Z_n^*\}$
For $n = p \cdot q$, where both are safe primes, and $p = 2r + 1$ and $q = 2q + 1, |Q_n| = r \cdot s$ and Q_n is cyclic.

7 Discrete Log Problem

Definition 8. $\forall$ *prime* p, g *is a generator of* Z_p^* *if* $order_p(g) = p - 1$

$$\log_{g,p}(y) = x$$

Here, x is the discrete log of y base g mod p. In other words,

$$y = g^x \mod p$$

Thm 3. *It's computationally hard to find* x *given* y *and* g. *(Discrete Log Assumption)*

8 Public Key Setup

- p: large prime (1024 bits)
- g: generator of Z_p^*
- Secret Key: $x \leftarrow \{0, 1, ..., p-2\}$
- Public Key: $y = g^x \mod p$

Security of secret key x follows from the DL Assumption.

9 Diffie Hellman Key Exchange

Secure way for Alice and Bob to exchange keys through a channel that has a passive adversary Eve (Eve can only listen; cannot send false message) eavesdropping.
Let G be a cyclic group with generator g. Both G and g are public.
Protocol:

1. Alice sends g^a publicly to Bob.
2. Bob sends g^b publicly to Alice.
3. Alice can compute $K = (g^b)^a = g^{ab}$. Bob can compute $K = (g^b)^a = g^{ab}$.

10 Decisional Diffie Hellman Assumption (DDH)

Given g^x and g^y, cannot distinguish g^{xy} and g^u w/ prob. $> \frac{1}{2} + \lambda$, where $u \leftarrow \{0, 1, ..., |G| - 1\}$
$\implies$ **Assuming DDH, Diffie Hellman is secure under a passive adversary.**

How to trick Alice and Bob (given that Eve can now intercept messages):

1. Eve intercept g^a from Alice and g^b from Bob.
2. Eve sends g^e to both Alice and Bob.
3. Alice thinks that K is now g^{ae}, and Bob thinks that the key is g^{be}. Even can now trick Alice into thinking that she's Bob, and vice versa.