# 4/23/18 Class Notes

Manish Joshi

May 7, 2018

This is a test.

## 1 Discrete Logarithm Problem

Suppose $\alpha = \beta^x$ (mod p)

If you know $\beta$, x, p,then computing $\alpha$ is easy with modular exponentiation. Now, Suppose you know $\alpha, \beta$, p and want to find x. How would you do it?

$a = b^x$

$ln(a) = xln(b)$

$x = \frac{ln(a)}{ln(b)}$

But, in modular arithmetic there is no analog of the $ln$ function, so this this method does not work. No one knows a fast way to do it.

Naive way: Brute Force: try all possible values for x until you find the one that works. This has a running time of O(p).

### 1.1 Diffie-Hellman Key exchange

Diffie- Hellman key exchange is an application of the discrete log problem which allows Alice and Bob to agree on a key securely over the internet, but they cannot use it to send messages.

Steps for Diffie-Helman

- Alice picks a large prime number, p ( 200 digits) and a primitive root $\beta$(mod p)

* Note: Primitive root powers produce every residue (mod p).

Everybody knows p and $\beta$

Alice picks a secret number a, 2 $\leq$ a < p-1

Bob picks a secret number b, 2 $\leq$ a < p-1

Alice computes $\beta^a$ (mod p) = A and sends it to Bob

Bob computes $\beta^b$ (mod p) = B and sends it to Alice

Alice computes K $\equiv \beta^{ab} \equiv B^a \pmod{p}$

Bob computes K $\equiv \beta^{ab} \equiv A^b \pmod{p}$

They use the first 128 bits as the key for AES or other encryption system.

## Why is this secure?

Eve knows p, $\beta$, A and B. She doesn't know a and b, and finding them requires solving the discrete log problem.