

## Math 110 In-Class Discussion

### April 28, 2005

In this document, we perform some computations based on the discrete log problem. We begin with a very small example of Diffie-Hellman key exchange.

```
parisize = 4000000, primelimit = 500000
(08:27) gp > znprimroot(29) \\ PARI command for primitive roots
%3 = Mod(2, 29)
(08:27) gp > znprimroot(47)
%4 = Mod(5, 47)
(08:27) gp > g=%
%5 = Mod(5, 47)
(08:28) gp > g^(18) \\ Person A picks a random number 18
%6 = Mod(2, 47)
(08:28) gp > g^7 \\ Person B picks a random number 7
%7 = Mod(11, 47)
(08:28) gp > Asecret=Mod(2,47)^7 \\ This computes g^(18*7)
%8 = Mod(34, 47)
(08:29) gp > Bsecret=Mod(11,47)^(18) \\ So should this.
%9 = Mod(34, 47)
```

Here's a one-line routine for finding the solution to a discrete log problem.

```
(08:30) gp > disclog(x,g,i) = i=g; for(n=1,znorder(g),
    if(x==i, return(n), i=i*g)); 0;
(08:34) gp > p=nextprime(10001)
%12 = 10007
(08:35) gp > znprimroot(10007)
%13 = Mod(5, 10007)
(08:35) gp > g=%
%14 = Mod(5, 10007)
(08:36) gp > random(10007)
%15 = 3188
(08:36) gp > a=g^(3188)
%16 = Mod(9086, 10007)
(08:37) gp > disclog(a,g) \\ To recover the exponent 3188
%17 = 3188
(08:37) gp > ## \\ But even with this simple program, it isn't secure.
*** last result computed in 20 ms.
```

Let's do a bigger example:

```
(08:37) gp > p=nextprime(12345678910)
%18 = 12345678923
(08:38) gp > g=znprimroot(p)
%19 = Mod(2, 12345678923)
(08:38) gp > k=random(p)
%20 = 897228705
(08:39) gp > a=g^k
%21 = Mod(9316966432, 12345678923)
(08:39) gp > disclog(a,g)
^C *** user interrupt after 28mn, 54,470 ms. \\ Tired of waiting...
(09:08) gp > znlog(a,g) \\ PARI's super duper solver
%22 = 897228705
(09:09) gp > ## \\ Yikes!
*** last result computed in 660 ms.
```

What is the state of the art? In finite fields whose size is a power of 2, the discrete log problem can be solved with significant effort for fields of size  $2^{521}$  according to a paper from 2001 on the number theory server. But the problem is significantly harder for primes other than 2.