

Re: find $(n-1)/2$ is prime

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-09/msg00973.html>

- *From:* "Joseph Ashwood" <ashwood@xxxxxxx>
 - *Date:* Wed, 27 Sep 2006 10:07:52 GMT
-

<andwing@xxxxxxxx> wrote in message
news:1159346569.421047.273120@xx

For realization of deffie-hellman it is required $g^{\text{rand}x} \bmod n$
n is prime.
How I can find prime number n, $(n-1)/2$ is prime too?
My computer has touched already more than 10000 numbers,
but $(n-1)/2$ does not pass the test of Miller-Rabin

The straightforward answer is to find prime $(n-1)/2$, then check to see if n
is prime.

The most complex answer which will be faster and deliver security that is
the same is to pick a prime q such that it is 1 bit shorter than your
desired security, then find k such that $k*q+1$ is prime, $n = k*q+1$. This will
be much faster then the other method, and should be of at least the strength
of the other methods. Note that method 1 is simply this method where $k=2$.

A variation on the second method is actually used in the creation of DSA
signing groups, where q is noticably smaller (160, 256, 384, or 512 bits)
with a significantly sized k (a few hundred bits). This method is even
faster, and knowing such a q makes it useful for DSA signing as well.

Any of these should work sufficiently faster than picking n and checking to
see if $(n-1)/2$ is prime. Also 10,000 is not necessarily a bad number of
primes to go through. You might also consider choosing prime p and checking
to see if either $(p-1)/2$ or $2*p+1$ is prime, this may speed things up even
more for method 1.

Joe

.