

Re: Parameters for Diffie–Hellman–Merkle

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-06/0153.html>

From: Gregory G Rose (ggr_at_qualcomm.com)

Date: 06/09/03

Date: 9 Jun 2003 09:01:43 -0700

(answering two messages in one, because I never got the one in the middle from Paul...)

In article <bc1ak7\$1hc\$5@titan.btinternet.com>, Richard Heathfield <binary@eton.powernet.co.uk> wrote:

>Paul Crowley wrote:

>

>> ggr@qualcomm.com (Gregory G Rose) writes:

>>

><snip>

>>

>>> *There's no reason at all for Y to be large.*

>>

>> *How do you go about finding a small generator of the order- q subgroup?*

In the case where $P=2*Q+1$, just try $g=2, 3, 4, \dots$ until you find one such that $g^Q \equiv 1 \pmod P$. It won't take long, because it is true for about half the elements.

In the case where you chose a 160-bit (or other size) Q , I'm not aware of any way to come up with a small generator, but if there is one, it would work fine. So I wasn't actually trying to say that it *should* be small, merely that this is one case where size doesn't matter. As for finding one, choose a random element "a" (may as well start with 2), and calculate $g = a^{(P-1)/Q} \pmod P$. If $g \neq 1$ then it's a generator of the order Q subgroup. If it is, try again with a different a.

>*In fact, what do you actually /mean/ by "order- q subgroup"?*

Well, you know what a group is, right? CAIN and ABEL: Closure, Associative, Identity, iNverse, and Abelian (Commutative). So, within the big group (the Multiplicative Group modulo P), there

