

Re: SF: Back to theory

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-02/9882.html>

From: Tim Peters (tim.one_at_comcast.net)

Date: 02/27/05

Date: Sun, 27 Feb 2005 14:11:55 -0500

[Tim Peters]

[...]

>> *I want to elaborate on that, because some results may be artifacts of the way primes are chosen. I pick an N -bit prime like so: pick a random integer i uniformly from the range $2^{*(N-1)} \leq i < 2^{*N}$, and then find the smallest prime $\geq i$. But not all primes in range are equally likely to get picked -- due to the way I'm choosing them, the probability of picking a particular prime p is proportional to $1 +$ the number of composites immediately preceding p . I can't imagine why that would bias the results, but can't swear that it doesn't. Another thing to test, anyway.*

[Mike Kent]

> *I believe you can get rid of (much of) the bias by modifying your procedure as follows:*

>

> *Pick a fixed number K with $0 < K < N$.*

>

> *Pick i between $2^{*(N-1)}$ and 2^{*N} as before. Make a list of the primes between i and $i+K$. If the list is empty, pick a new i and repeat; otherwise randomly pick an item from the list.*

>

> *Picking $K = 0$ gets rid of all the bias -- the modified procedure then amounts to pick i , see if it's prime. $K = 1$ is almost as good since only one of i and $i+1$ is even. As K gets larger, bias arises against primes that occur in clusters (the items of a prime pair are roughly $1/2$ as likely to be picked as is a prime with not near prime neighbors, for instance); as K decreases, the expected number of iterations increases.*

Those sound like good ideas, and I'll keep them in mind. The numbers we're testing here so far are still so small that it's thoroughly practical to precompute a list of all primes in range, and just pick elements at random (uniformly) from that list. I changed the code to do that, but too early to tell whether it matters to the results (3% of a test run has finished, and there's clearly no dramatic change so far).

sci.math: Re: SF: Back to theory

OTOH, this is a small-scale dumb-ass approximation to how RSA primes get chosen, and I expect that most methods for that in practice work more like my original scheme; e.g.,

<http://eprint.iacr.org/2003/186.pdf>

On the third hand, my goal right now is to understand the better-than-random results, and picking primes truly at random (well, within the Mersenne Twister's likely-irrelevant limitations) takes one possible source of bias out of the picture.