

Re: Surrogate factoring code

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-06/2136.html>

From: Tom St Denis (*tomstdenis_at_iahu.ca*)

Date: 06/29/04

Date: Tue, 29 Jun 2004 15:04:04 GMT

James Harris wrote:

- > *Like with tiny numbers like 23(79) or 131(101) it factors basically*
- > *immediately in a single iteration, but with slightly bigger numbers,*
- > *still tiny, it's not a lot either, compared to random, like*
- > *9497(9689)=92016433 factors after 51 iterations.*

With pollard-rho that would factor in ~90 steps on average. I don't think one iteration of yours is enough to determine if it's an average.

So basically what you are saying [extrapolating here] is at best your method is 2x faster than pollard-rho. However, still quite a bit is lacking such as a complete working description of the algorithm with some idea of the big-Oh complexity.

Tom