

Re: JSH: Nearly done

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-01/7906.html>

From: David Kastrup (dak_at_gnu.org)

Date: 01/27/05

Date: Thu, 27 Jan 2005 02:10:27 +0100

jstevh@msn.com writes:

> *I'm focusing on building a full method that relies only on my work,*
> *so it has to call itself recursively to factor, and such a method*
> *can potentially chew through even an RSA challenge type number in*
> *minutes.*

Nonsense.

> *Then it's just a matter of iterating through the various*
> *combinations, which I've figured out are at about 150 million for*
> *the number generated by the first 1000 primes.*
>
> *Potentially this method can factor an RSA challenge sized number in*
> *seconds.*

The RSA challenge numbers are a far cry from being in the ballpark of the first 1000 primes.

> *I call that polynomial time.*

In short: you are completely talking out of your ass. You are throwing around runtime numbers which are not based on any actual runs, you are throwing around success rates that are not based on actual data, and you are throwing around buzzwords for which you have no clue about the meaning.

--

David Kastrup, Kriemhildstr. 15, 44793 Bochum