

Re: unprovability of the security of computational cryptography

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/1496.html>

From: Mack (macckone_at_a_nospamjunk123_ol.com)

Date: 10/13/03

Date: Mon, 13 Oct 2003 12:16:42 GMT

On 12 Oct 2003 23:05:25 +0300, Phil Carmody
<thefatphil_demunged@yahoo.co.uk> wrote:

>Mack <macckone@a_nospamjunk123_ol.com> writes:

>

>> On 11 Oct 2003 19:06:55 +0300, Phil Carmody

>> <thefatphil_demunged@yahoo.co.uk> wrote:

>>

>> >Bryan Olson <fakeaddress@nowhere.org> writes:

>> >> D. J. Bernstein wrote:

>> >...

>> >> > (i) Factoring 512-bit numbers will be infeasible for the next ten

>> >> > years.

>> >...

>> >> The 'evidence' for the first is a curve of the size of numbers

>> >> really smart people have figured out how to factor, plotted

>> >> against time, and extrapolated. It's more than a little sketchy

>> >> now, and if a $P=NP$ bombshell drops, that extrapolation becomes a

>> >> joke.

>> >

>> >Why?

>> >

>> >Phil

>>

>> Would not a proof that $P=NP$ involve showing that at least one

>> NP complete problem can be definitively solved in P?

>>

>> From what I remember an algorithm for solving one problem can

>> be used to solve other problems. The conversion may not be

>> simple but it would change the way we look at factoring.

>

>Would it necessarily change the way we look at factoring

>512 bit numbers? That was the problem in hand.

>

>For example, let's say I had a $\Theta(\text{digits}^{100})$ -time

> $\Theta(\text{digits}^{50})$ -space (with constants ~ 1) deterministic

sci.crypt: Re: unprovability of the security of computational cryptography

> *factoring algorithm. What are you going to do with it. What*
> *_concretely_ will have changed. Would you use my method or*
> *would you stick to solutions like NFSNet, or Twinkle-alikes.*
>
>> *Proving that a polynomial time factoring method exists would*
>> *probably lead directly to such a method.*
>
> *I think you're missing the point.*

That is why I asked the question. I see what you are saying.
If the polynomial time algorithm is slower than the non-polynomial
time algorithms already in place for numbers of the size in
question then it would not be significant.

>
> *Phil*

Leslie 'Mack' McBride
remove text between _ marks to respond via e-mail