

Re: Surrogate factoring demonstrated

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/4622.html>

jstevh_at_msn.com

Date: 02/26/05

Date: 25 Feb 2005 16:16:01 -0800

jstevh@msn.com wrote:

> *jstevh@msn.com* wrote:

>> *I think it'd help to show an actual example of surrogate factoring,*

>> *which of course is a picked example, of a case where it works.*

>>

>

> *I'm still working on the algorithm and seeing what it will factor.*

>

> *Here's one I just did.*

>

> $M = 116565983987934769$

>

> $T = 1331674354105829165393067963530771325$

>

> T^6 factored is

>

> $(3^{18})(5^{12})(89^6)(479^6)(137573^6)(214213^6)($

> $146655731^6)(10707563851^6)$

>

> *Iterations: 555547*

>

> *Max is 8 times that or 4,444,376*

>

> *Time/iteration: <deleted>*

> *Number factored.*

> *Initial Factorization:*

> $f_1=247816937$

> $f_2=470371337$

> *Now checking its factors...*

> *moving up a level*

>

> *Success!*

> *Factors:*

> $(247816937)(470371337)$

> *Product: 116565983987934769*

>

> *In coming is 116565983987934769*

> *Processing time: <deleted>*

- > *Number of digits: 18*
- > *bitLength=57*
- >
- > *I'm still working on my idea about blocking primes, so I'm forcing in*
a
- > *factor of 15 into T.*
- >
- > *I'm trying to find a number the current algorithm does NOT factor.*

Well, found it. Sigh. I'll tell you the trouble with ideas, there's little worse than coming up with something new.

So I have this idea that I think is worth checking into, which is to use some other number to factor a target, and I can get some tantalizing results but I can't nail it all down, so I have to go into long-term research mode.

Some posters seem to think it's worth their time to try to convince you one way or the other about this method, but they don't know what I know.

It doesn't matter.

New ideas don't get picked up rapidly.

People don't steal great ideas.

They run away from them.

I made a post about how surrogate factoring is a concept—you use one number to factor another—but it won't stop posters from telling you it can't work, even though it's a concept, so how can you say it can't work.

But again, it doesn't matter. They're wasting their time, as people don't latch onto new ideas rapidly. You don't get cheered. You don't have people congratulating you on your creativity.

You get called a crackpot.

Years pass, maybe even decades, and then you're hailed as brilliant, often after you're dead.

That's what being a discoverer is today, as it has been for some time.

I think it has to be that way with humanity.

Like, it's built into the genes.

No one breaks those rules, and people you think did, history will show were not who *you* thought they were, as much of what people think they

sci.crypt: Re: Surrogate factoring demonstrated

know, is what they're told, and you know what?

People can *say* just about anything.

James Harris