

Re: JSH: What if I succeed?

Source: <http://sci.tech--archive.net/Archive/sci.math/2007-08/msg04764.html>

- *From:* Rupert <rupertmccallum@xxxxxxxxxx>
 - *Date:* Mon, 27 Aug 2007 21:09:19 -0700
-

On Aug 27, 2:41 am, JSH <jst...@xxxxxxxxxx> wrote:

For years I've been talking about using the factoring problem to force acceptance of my other mathematical research as I figured that if I demonstrate my problem solving ability with a practical math problem away from "pure math" then I can get people to pay attention to my other decried research.

My take on responses from this newsgroup at least has been a contemptuous dismissal of any possibility of my success.

There's a fairly strong chance you won't succeed, yes. But that's no reason why you shouldn't try. You don't seem to be willing to put much effort into it, however. Why don't you review the literature and see what other approaches people have tried?

But what if I succeed?

Well, that'll be great. We'll have an interesting new mathematical result, and we'll have to use some other form of public key cryptography.

The scary part to me is not the world's markets but the possibility that the academic math world IS as dumb as I've feared as if I just trot out a solution that shows that factoring is a trivially easy problem, and do it with ideas I've talked out over a year, how can it be smart?

I'm not sure I understand your concern here. If you succeed you should be able to produce irrefutable evidence that you've succeeded. It won't matter whether the mathematical community is smart or dumb

Re: JSH: What if I succeed?

(though you've got no reason to think it's dumb). People will announce that the RSA cryptosystem is no longer secure, and people will start using other forms of cryptography.

Especially if it has spent the last five years ignoring my proof of FLT and my prime counting function along with other research?

There's a very good reason for that.

And, um, can I ethically present a stunningly simple proof of how to make my latest "surrogate factoring" approach work at a time like this when the world's financial markets are already on edge?

It's very simple. You make a public announcement that the RSA cryptosystem is no longer secure and demonstrate that you can crack it. People thank you for the information and make arrangements to use other forms of cryptography. After the transition period is over, you publish the algorithm. No ethical problem involved.

But where can I go with the research?

I've already contacted the NSA in the past when I was wrong, and I've bugged cryptology people over the years, so how do I go to anyone now?

If you succeed, you will be able to write code that can efficiently factor large numbers and it will be easy for people to verify that this is the case. Set up the code on a secure server and let people check that it works, without revealing the actual code until they have had time to adjust to the situation.

But more importantly, how can it be so trivial?

Well, it would certainly be very strange if the problem were as easy as you're hoping it is. Is there the tiniest chance you're mistaken about that?

How could R, S and A present something so pathetically easy to solve to the world as a security system, and manage to convince people?

Re: JSH: What if I succeed?

Re: JSH: What if I succeed?

Yes, something funny's definitely going on. Could it be we're making any questionable assumptions here? I wonder what they are. Beats me.

Should I hide math for the good of financial markets to protect a math culture that seems to be stupid on a scale hard to comprehend about even the most basic mathematics?

No. If you can write code that can factor numbers efficiently you should announce the fact.

Or let fly? I think I have no choice but to simply present the research and let the chips fall where they may because the situation is so unprecedented that there is no rulebook.

So, let me get this straight here: is there something you've achieved that you haven't already presented in a public forum? When you've actually got a new "achievement" that you haven't announced yet, then you can start worrying about the ethical dilemma of what to do. I wouldn't have thought it would be too hard to release the information without causing anyone too much inconvenience.

There simply is no right answer.

James Harris