

Re: JSH: So what do we do now?

Re: JSH: So what do we do now?

Source: <http://sci.tech-archive.net/Archive/sci.physics/2008-01/msg01436.html>

- *From:* JSH <jstevh@xxxxxxxx>
 - *Date:* Sat, 19 Jan 2008 09:29:31 -0800 (PST)
-

On Jan 19, 8:55 am, Randy Poe <poespam-t...@xxxxxxxx> wrote:

On Jan 19, 11:18 am, JSH <jst...@xxxxxxxx> wrote:

On Jan 18, 6:54 am, Randy Poe <poespam-t...@xxxxxxxx> wrote:

On Jan 17, 8:14 pm, JSH <jst...@xxxxxxxx> wrote:

The alternative is a very public demonstration, like factoring RSA public keys in posts on this newsgroup, but I project that afterwards stock markets around the world would crumble, and what's happening now with them would look like the good 'ol days.

A convincing and perfectly safe demonstration would be to factor RSA challenge numbers that have already been factored, such as RSA-140.

Go for it.

Another convincing demonstration would be to factor some small primes, say of 4, 5, ..., 9 digits, and give us run times for your algorithm to show us how it scales. Then we could project that up to hundreds of digits.

Re: JSH: So what do we do now?

The advantage of using 9 and fewer digits is that you don't need to use an arbitrary-precision library, you can use your built-in integer types.

Hint: If you find that your factoring of an RSA key is projected to take 100 orders of magnitude more than the age of the universe, then world civilization won't end. We already know it's possible in principle to factor these keys. Their safety lies in the fact that it takes more time than anybody has to do so.

– Randy

Seemingly reasonable suggestions that ignore the realities of the situation.

For those who think that is a dodge,

It's a dodge.

I've simplified a bit to get a result that looks more directly related to factoring, where the point I want to make is--these are fundamental relations.

Are they applicable to factoring? Have you "solved the factoring problem"? Can your "fundamental relation" make any difference whatsoever in the time it takes to factor large primes?

Prove it: Factor one.

– Randy

There is no factoring outside of the rules shown by the factoring congruences.

So even what factoring that is done today by other methods like the Number Field Sieve is within that framework.

Re: JSH: So what do we do now?

Re: JSH: So what do we do now?

The point I'm making now is that even with absolute evidence from mathematical proof, in a system easily explained, math people keep trotting out the only thing left to deny overwhelming evidence which is to demand that I personally factor some large number.

As I've pointed out before, it's like if physicists had told Einstein to build an atomic bomb before they'd believe him about this relativity nonsense!

Math people have changed the rules, yet again. Just like when I was published in a peer reviewed mathematical journal.

I'm not the one making the doge. The math community is.

It has now backed down to a corner where it's saying I have to be the one to demonstrate, but with fundamental mathematics, why wouldn't someone else exploit it?

To math people who are used to getting away with denial the simple notion that someone else in the world would exploit the mathematical ideas is foreign to them.

They won't believe it until they see it. Just like they won't believe mathematical proof until someone demonstrates it works.

Like they won't believe in anything until it explodes in their faces, as if physicists had denied Einstein until the first atomic bomb was exploded and a bunch of them went with it as they were sitting on top of it with their arms crossed saying it wouldn't work.

James Harris

.