

Re: New way to factor? Yes!

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-02/2765.html>

From: Décio Luiz Gazzoni Filho (*decio_at_decpp.removethis.net*)

Date: 02/09/05

Date: Tue, 08 Feb 2005 22:51:53 -0200

Richard Cavell wrote:

> On 8/2/05 11:34 PM, José Carlos Santos wrote:
>> Dave Turner wrote:
>>
>>> I love crypto but i'm a just part-time amateur, everything you've said
>>> is beyond what most of us can understand, so my question is:
>>> If somebody gave you a large prime number, could you factor it? Wouldn't
>>> doing so shut your critics up? :-)
>>
>>
>> Give me **any** prime number, as large as you want, and I assure you that
>> I can factor it! :-)
>>
>
> Go to *rsasecurity.com*. There's a competition there worth a few hundred
> thousand US dollars to factor some big numbers. Go make some money.
> Also, Microsoft's X-box has a 2048 bit RSA key that some people want to
> see broken. That's worth \$10,000.
>
> This is the easiest way to shut your critics up, and to buy yourself a
> Mercedes as compensation.

Uhh... he's talking about prime numbers. Prime numbers, by their very definition, have only a single non-trivial factor, namely themselves. These numbers you speak of are composites. Specifically, they're the product of two smaller (yet still very large) prime numbers. Those are indeed very difficult to factor, as far as we know. However, José never mentioned composites, so what you're saying doesn't apply.

Décio