

## Re: Surrogate factoring, a fascinating idea

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-06/0742.html>

---

**From:** Douglas A. Gwyn (*DAGwyn\_at\_null.net*)

**Date:** 06/11/04

Date: Fri, 11 Jun 2004 12:30:30 -0400

James Harris wrote:

> *It IS a little problem, mathematically.*

I have to agree with him there.

However "theoretically" unimportant, it still is important for getting Mr. Harris the public recognition that he so obviously craves. But in that case, the missing detail (choice of s) deserves whatever work it takes him to fill in.

> *But you people didn't do that and you in particular mainly called me > names.*

Don't mistake Tom StDenis for "you people". You should respond to the best criticism, not to the worst.

> *I've done all that I need to do mathematically to prove my case.*

What specifically \*is\* your case? If it is supposed to be that you have found a practical method of factoring large numbers, that has yet to be demonstrated. (Tell us how to efficiently find a workable value for s.)

> *I have a theoretical approach to factoring, which I think shows that > factoring is NOT a hard problem as previously thought.*

The idea of using the additional information (that the input number is known to have two factors) is not new; in fact I mentioned that as potentially exploitable many years ago, and I would be surprised if the same thought hasn't occurred to many other people. What would be \*useful\* would be for you to explain step by step how you went from the general problem "find factors" to the particular algorithm/formulas. I.e. how do you apply your general theory to arrive at a solution to the particular problem. If you do have some deep theory then what is it? Can you express it as a theorem using

sci.crypt: Re: Surrogate factoring, a fascinating idea

standard mathematical terminology so that it can be  
evaluated and applied by others?