

## Re: Critiquing surrogate factoring

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-03/2440.html>

---

**From:** Bruce Stephens ([bruce+usenet\\_at\\_cenderis.demon.co.uk](mailto:bruce+usenet_at_cenderis.demon.co.uk))

**Date:** 03/31/05

Date: Thu, 31 Mar 2005 10:09:08 +0100

jstevh@msn.com writes:

[...]

> *I will remind that what I presented here in my original post is a  
> theorem, and being a theorem, it's not arguable as to its  
> correctness.*

Ah. So your proof of the theorem is that it's a theorem, and is therefore true? That would be proof by assertion, I think  
<<http://www.enseeiht.fr/~queinnec/proof.html>>.

> *That theorem shows that you get rational factors of  $M^2$  from using  
> the factorization of  $Tj^2$ , where  $T = M^2 - j^2$ , and  $j$  is a number  
> you select, with the requirement that  $j^2 > M^2$ .*

It would probably help if you defined what you mean by a rational factor (or just give a reference; I couldn't see any definition online). Of course what we actually want is non-trivial integer factors of  $M$ . So even if the alleged theorem is true, it may be valueless for factoring in the usual (integer) sense.