

Re: Critiquing surrogate factoring

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-03/2396.html>

From: C. Bond (cbond_at_ix.netcom.com)

Date: 03/30/05

Date: Wed, 30 Mar 2005 20:38:08 GMT

C. Bond wrote:

> *jstevh@msn.com* wrote:

>

>> *The idea is simple enough, factor one number and use its factorization
>> to get the factorization of another. The point being taking a number
>> that is hard to factor, and yet, factoring it, by factoring an easier
>> number.*

>>

>> *I thought it might help to try and write the the gist of it in a
>> theorem.*

>>

>> *Surrogate Factoring Theorem:*

>>

>> *Given M , a target natural number to be factored, and j , an integer
>> chosen such that $j^2 > M^2$, a rational factor b_2 of M is given by*

>>

>> $b_2 f_1 = (- (Az - 2M^2) \pm \sqrt{(Az - 2M^2)^2 - 4TM^2}) / 2$

>>

>> *where $T = M^2 - j^2$, and f_1 is a rational factor of T , and where Az is
>> given by*

>

> *If $j^2 > M^2$, as required above, then T is negative. Is that what you want?*

Since James has apparently chosen not to answer this question, perhaps he will answer another. Does the statement " f_1 is a rational factor of T " mean that f_1 is *any* rational factor of T ? Or does it mean that f_1 is a particular rational factor T whose value is to be determined by some means? By the way, for completeness, what is your definition of a "rational factor"?

--

There are two things you must never attempt to prove: the unprovable -- and the obvious.

--

Democracy: The triumph of popularity over principle.

--

<http://www.crbond.com>