

Re: JSH: SF: Finally, surrogate factoring

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-06/msg00852.html>

- *From:* "Tim Peters" <tim.one@xxxxxxxxxxxxx>
 - *Date:* Mon, 5 Jun 2006 23:04:46 -0400
-

[added "JSH:" to subject, spared sci.crypt and alt.math]

[jstevh@xxxxxxx]

...
And it has been posted in this thread that I DID get it wrong.

If you do it right, it shows a dependency on the factorization of T,
which is no good.

But what if you go the other way, isolating y on the right side,
instead of z?

....

So instead, you would complete the square twice isolating z on the left
and with the second you would get y inside the square on the right.

The reason for wondering is that if you solve for z using the four
linear equations, yup, it does solve in such a way that you can have a
difference of factors of T, but y does not.

Long-shot.

I got

$$(42*z + 10*y - 3*f_2 + 19*f_1)^2 = (4*y + 3*f_2 - 5*f_1)^2 + 84*T$$

then, but didn't care enough to double-check it.

.