

# Re: JSH: SF: Finally, surrogate factoring

---

*Source:* <http://sci.tech--archive.net/Archive/sci.math/2006-06/msg01044.html>

---

- *From:* [jstevh@xxxxxxx](mailto:jstevh@xxxxxxx)
  - *Date:* 6 Jun 2006 18:20:07 -0700
- 

Rick Decker wrote:

Rick Decker wrote:

Tim Peters wrote:

[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.

Re: JSH: SF: Finally, surrogate factoring

Long-shot.

... and a miss.

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.

That's what I got, too. Mathematica agrees.

(Responding to my own post...)

So completing the square w.r.t y first yields

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

Completing the square w.r.t. z first yields

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

Hey, I was curious to see it, figured someone could put up a solution, and I guess you're right, but, let's think about it a bit.

If you are correct, then

$$4y + 3f_2 - 5f_1 = h_1 - h_2$$

where  $h_1 h_2 = 21T = 21 g_1 g_2$ .

But I can also solve for y directly using the 4 linear equations, expressing it directly as a solution of  $f_1$ ,  $f_2$ ,  $g_1$ , and  $g_2$ .

Given y