

Surrogate factoring, random is better?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/3413.html>

jstevh_at_msn.com

Date: 02/18/05

Date: 17 Feb 2005 15:27:09 -0800

I keeps seeing posters claiming that my surrogate factoring method is worse than even chance or at best only as good as a chance method for factoring.

There are several problems with their assertion.

That is, I suggest that they are lying. Here's why.

The base equations are

$$yx^2 + Ax - M^2 = 0$$

$$yz^2 + Az - j^2 = 0$$

and

$$T = M^2 - j^2$$

from which you can easily find

$$Ax = Az(-Az \pm \sqrt{(Az - 2M^2)^2 - 4TM^2}) / (2j^2 - 2Az)$$

$$Az = Ax(-Ax \pm \sqrt{(Ax - 2j^2)^2 + 4Tj^2}) / (2M^2 - 2Ax)$$

where I've basically wrapped up all the unknowns.

You give M, as it's the target, and j, as it's some picked integer, and then everything else gets determined.

Well you have *two* base equations showing x, y, z and A are the unknowns, and then I substitute out y and wrap A up with x and z, so you have Ax, and Az as unknowns.

Substituting out y, gives you the two equations defining Ax and Az, where the final constraint is the rationality of the square roots.

Now from the first equations square root there MUST be a rational Az that factors M, so there must exist Ax, and Az such that M is factored.

Surrogate factoring, random is better?

That's a crucial point, and the first clue that posters must be lying, as now you have a system where the factorization of M , the target, must exist, for some solution.

I noted that Ax an integer doesn't usually work, as that's the basic approach I tried before, and I agree that it gives a low probability of success, but first thing to note, which CANNOT be disagreed with, there is a rational Ax that MUST work.

So now you have an issue with the value of that Ax , as you might have

$$Ax = n/m$$

where n and m are integers.

Well, suddenly you have *two* more variables, in a system that up until now has been fully constrained, as you had three unknowns with two equations, where the final constraint is a rationality of square roots constraint.

So guess what?

If posters claiming my method doesn't work are right, then m is basically a random number.

My method then would be the world's first perfect non-quantum random number generator.

If m is NOT random, then there is some mathematical reason or constraint that governs the value of m , and then that can be determined and if you figure it out, then you have a solution to the factoring problem.

So, either I've found the world's first perfect, non-quantum, random number generator, or there's a way to make this method work.

I suggest to you that posters are not so dumb as to not realize the constraints and reality here, but are actually deliberately lying about what follows mathematically, for their own reasons.

Now I did the analysis that shows that in fact the denominator of Ax IS in fact determined so that it contains prime factors of T .

The math is not hard proving this fact.

Now then, I would be curious if any poster might reply explaining how there is some other possibility than I mentioned:

1. A perfect random number generator
2. A method that must work in some deterministic fashion.

sci.crypt: Surrogate factoring, random is better?

If and when they dodge those possibilities, trot out crap to try and explain why that is not valid, without giving anything *mathematical* then you will know that yes, they are indeed, lying.

James Harris