

# Surrogate factoring, out of the box

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-01/2570.html>

---

*jstevh\_at\_msn.com*

**Date:** 01/29/05

Date: 29 Jan 2005 12:09:31 -0800

Well I'll admit that I've been feeling a bit depressed the last couple of days, as I had calculations showing at least 50% success with a rational  $x$ , and then I checked thoroughly and found that my method gave a LOT of rational  $x$ 's, and wasn't factoring with most of them.

And then I realized that for most cases it gives you an  $x$  that has your target itself as the factor.

I puzzled over that result, and realized that the math was too efficient in searching through rational solutions, so that it could, most of the time, find solutions such that the target itself was the factor of  $x$ , hence my problem.

So I squared the target, and it factored.

Why? You need to understand quadratic residues to understand why.

Basically the probability was too high that it could get quadratic residues for both of my factors, so by squaring them, I forced the math to look for solution for those factors squared, making it more likely that it would fail for at least one, and it did.

I have verified that the value of  $A$  is mostly irrelevant, except with regard to evens, as either you need  $A=8$ , or maybe you might do well by making  $A$  a fraction and using  $A=1/2$  or  $A=1/4$  or  $A=1/8$ , which I say as I haven't checked it, as I now just use  $A=8$ .

That issue has to do with allowing rational solutions based on balancing out evens versus odds with

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

as  $M$  is usually odd, so if you don't make  $A$  even, and at least 8, then you'll get situations where  $y$  and  $x$  can't be rational, as they want to be odd, but if  $A$  is odd, then you have three odds trying to add up to 0, which can't work.

## sci.crypt: Surrogate factoring, out of the box

I'm still puzzling over the quadratic residues a bit, as it's not to the prime, as I first thought, but to the prime squared. So like if 5 is a factor of M, then the quadratic residue result has to do with

$$d_1^2 = w_1' w_2 \pmod{25}$$

not mod 5, as I thought originally.

Oh, the quadratic residue result is

$$d_1^2 = w_1' w_2 \pmod{g^2}$$

where g is a prime factor of your target, and d\_1 is what is picked for you by the math as it checks through all integers to see if a d\_1 exists.

$$w_1 w_2 = j^2 T$$

and I'm using w\_1' for the modular inverse of w\_1.

So yeah, the factorizations of j AND T play a role.

That's the profoundly fascinating feature of this method, as infinity itself is checked for results!

And that is rigorously proven.

I just didn't realize that more than likely it will find d\_1, out of infinity.

Well, infinity is kind of big...

So yeah, if you try to factor something not prime, and get no factors, square it.

I've updated the Yahoo! site:

<http://groups.yahoo.com/group/sufactor/>

and I'm going to work on settling down the probabilities, as I find it curious.

So even I got stuck thinking inside of the box, as I kept puzzling over why I didn't get what I wanted—a solution—versus paying attention to this flood of rational x's that had M^2 itself as a solution, in defiance of my earlier quadratic residues results, which was just off. Fun. Math is great.

James Harris