

Reality check, surrogate factoring

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-01/1964.html>

jstevh_at_msn.com

Date: 01/26/05

Date: 25 Jan 2005 18:36:47 -0800

Already certain posters have made it their business to corrupt information to the point that some may be confused about how surrogate factoring works.

These mad little demons who obsessively reply to my posts make it their business to lie about the details, or even the big stuff. Don't ask why, they just do.

So, here's a post to just go over the facts, and mention why you should not decide that just because I have a prototype that doesn't *seem* to work well that there's nothing to this method.

Surrogate factoring is meant to beat the tactic of picking two hard primes to get a number hard to factor by allowing you to simply shift to a different number which you factor, the surrogate, to factor the original number, indirectly. The surrogate, of course, is not carefully picked to be hard to factor. But you do have to factor it, and it will be really big for a big target.

You still have to directly factor something.

But, you're factoring T , where $T = M^2 - j^2$, where M is your target, and j is picked. Like typically j is odd, as M is odd (though you may need to make it even, more later), and you can also pick j such that T is divisible by 3, or such that it is divisible by any number you wish it to be.

You also get a partial factorization of T at the outset as

$$T = (M-j)(M+j)$$

so what I'm saying is that some people somewhere work really hard to pick p_1 and p_2 so that $p_1 p_2$ is hard to factor by known methods, and surrogate factoring allows you to blow all of that out of the water by shifting to another number, easy to factor.

Ok, so that's what's in the algorithm and in the math already posted.

sci.crypt: Reality check, surrogate factoring

The information is already out there how to do the surrogate factorization.

There's only been one major bump along the way from my perspective in working out the theory as well as trying to SEE it work as I found that my prototype implementing the method didn't factor 100% of the time.

I had figured that it should for some simple mathematical reasons.

That's when I started posting to try and figure out what might have been an idea-killer, and I ran into quadratic residues which were forcing the method to work 50% of the time for *each* rational x found.

To understand the details you need to read the paper, or some of my posts going into details.

So what's the bottomline?

Well, I'm not sure about how to get rational x 's, but right now, not hypothetically, but mathematically proven, if you take any number that you can factor a T with, and get some rational x 's (non-trivial ones as there are dumb ways to get trivial ones) then you have a 50% chance of factoring the number.

The big question here is, can you find rational x 's?

My research indicates that you can be blocked from rational x 's by factors of 2, so that if what I've worked out is correct--not sure yet--then you just multiply your target by 2^n , where n is some positive natural number, and for some n you'll get a rational x .

If so, then that's it. Problem solved.

If that is true, then yes, someone right now, using standard tools can shift a factorization of a hard target to factoring a surrogate and use the surrogate factorization to break the target up.

The only significant question is, can you get rational x 's?

So then, why don't I just use my own wonderful theory to crack really big numbers?

I need to factor really big T 's.

And I just don't feel like trying until I have a handle on the theory.

Like, I could go to a lot of trouble to try and factor some RSA challenge number and sit there fiddling with things, waiting days for it to work out with some tweaks to my prototype (yes, I can make it faster, and no I'm not going to talk about how) and then find out that I just can't get rational x 's, and not know why.

Reality check, surrogate factoring

I figure I'll work out the theory first.

Now then, if someone wishes to argue with me on the mathematics, one thing they can do is attack the calculation showing the quadratic residue result.

If you're into implementation, you can show that it doesn't factor 50% of the time for rationals x 's.

Now if this idea does work, it seems likely that *someone* out there may at some point get motivated to check the theory or just check and see if it works like I say. If they get rational x 's then they will be able to factor VERY large numbers, VERY quickly.

The information is already out there. The software tools are readily available, and all it takes is someone who just checks just for the hell of it—if it works.

My guess is that it could take at most a month, but I figure it should have happened by now, so maybe the thing won't work, you know?

But, even if it doesn't work, I'm happy as the math is neat. I can write papers on what I already have verified.

It'd make a neat paper just to figure out why it doesn't work!!!

It's great fun, I'm having a great time, when not worrying about the world, and I've quit worrying about the world, so I'm having great fun.

Now if you look over the math, and understand it, you will be terrified, as it says this idea will work, and right now anyone with the tools and the will can factor some HUGE numbers, like FAR huger than you would want to imagine.

But, then again, maybe no one will check, and no one will test just for the hell of it, and we're safe just because...you know?

James Harris