

SF: National security

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/1965.html>

jstevh_at_msn.com

Date: 04/28/05

Date: 27 Apr 2005 16:34:11 -0700

Now I'm going to lay it out on the line, as I think this has gone on for a lot longer than I ever thought possible.

The SFT is not a joke, and it is now freely available, which has national security implications.

The longer policymakers are unaware of it, the worse things may be.

The SFT gives the solution to

$$\sqrt{x^2 - 4A^2(A^2 - B^2)y^2}$$

with all integers, where A is the number to be factored and B is some number you pick to factor it, which need only be non-zero and coprime to A, while x/y is determined by the rational factorization of

$$B^2(A^2 - B^2).$$

Those of you who know a smattering of mathematics and some about cryptography can easily see that such a theorem has some real importance.

Some of you may think that it's in your best interest to work alone or in some group to develop a practical factoring method from the theorem, and maybe go after the RSA challenge numbers.

Well, even if you manage to factor them, and send that information in, what good is the money if you're in jail?

I'm mentioning national security for a good reason.

I'll make the case that those of you who are experts in this field who for whatever reason are sitting on your behinds or privately pursuing your own research are endangering the security of the American people, and it doesn't matter what you say later, or what argument you come up with, or what lawyers you may try to get, as you may not even get a public trial.

I need someone who can talk to the NSA to talk to them, as they will not listen to me, probably a lot because of this crackpot label some of you have so diligently worked to put on me.

Now I want you to think carefully.

You may think you know all you need to know. You may think you're safe in some country other than the USA, but when it's finally known what the SFT is, then I will be talking to the policymakers.

Think about it.

And remember, you may not even see a public court or get a phone call.

I need someone to contact the NSA, so that I can go and brief them on the situation.

And I can guarantee some of you who may even now be waiting on RSA, if someone has exploited the theorem, that before you ever see a dime you will be sitting in front of some people asking you some very hard questions.

James Harris