

Re: How long to break a 512 bit RSA key?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/3065.html>

From: Mxsmanic (mxsmanic_at_hotmail.com)

Date: 10/31/03

Date: Fri, 31 Oct 2003 11:19:48 +0100

Hyper4S writes:

> *I was wondering how secure 512 bit RSA keys are, and some "googling" showed
> me that "they can be broken".*

All RSA keys can be broken, in time. "Broken" means that the key can be discovered in a way that is more efficient than an exhaustive key search; in the case of RSA, the method used is factorization, which is considerably faster than a key search.

> *Moreover, it seems that this can be done rather *easily*, in a *reasonable*
> amount of time.*

It depends on what you consider easy.

> *But I couldnt figure out what's exactly meant by that "easily" and
> "reasonable".*

Well, cracking a 512-bit key currently requires executing about 250,000,000,000,000 machine instructions, using the most efficient algorithms. Divide that number by the speed of the computer(s) your adversary has available to determine how long a 512-bit key will hold out against cracking efforts.

When RSA's 512-bit public challenge key was cracked in 1999, it required almost four months and just under 300 computers. It could be done much faster today, but it still requires a lot of work. For example, with a PC at 3.3 GHz, for example, it would take about 2.5 years of continuous work to crack a 512-bit key. That's certainly technically feasible, but it's not very convenient, so the real question is whether or not your adversary is prepared to invest that much machine time in cracking your 512-bit key. If he is, your key may be unsafe (unless you only need secrecy for a period shorter than the period required to crack the key); if he isn't, you're completely safe.

> *So, what would it take to break a 512 bit RSA key? A massive network of
> high-end computers? A simple desktop pc? And how long would it take? 10
> seconds? More than a year?*

sci.crypt: Re: How long to break a 512 bit RSA key?

See above. With the fastest PC available, probably 2–3 years of continuous operation. With a network of such PCs, much less time, of course. The computer doesn't have to be high end; any computer will do. However, it's obviously preferable that the computer be as fast as possible.

> *How long would it take to break a 512 bit RSA key on, say, a desktop pc with 1 GB RAM and 3 Mhz processor speed?*

Almost 3000 years ... if you really meant 3 MHz (there haven't been any PCs that slow around in twenty years, though). If you meant 3 gigahertz, then it would be 1000 times faster ... which means about three years.

> *Could you refer to the words of some authority in this field, who has "proven" this? Some founded references?*

See <http://www.rsasecurity.com/rsalabs/challenges/factoring/rsa155.html>, which discusses the cracking of the 512-bit key.

Cracking a 1024-bit key, incidentally, requires about 230 times longer. No one has publicly done it yet (as far as I can recall).

--

Transpose hotmail and mxsmanic in my e-mail address to reach me directly.