

Re: RSA encryption/decryption

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-09/0761.html>

From: Milan VXdgsvt (milan_vxdgsvt_at_seznam.cz)

Date: 09/18/05

Date: Sun, 18 Sep 2005 19:19:56 +0000 (UTC)

Mxsmanic wrote:

> *Milan VXdgsvt writes:*

>

>> *For Mxsmanic: current factoring algorithms are more effective than
>> $O(\log(N))$. Increasing the length of the number to be factored by one
>> bit does not take 2x times longer anymore.*

>

> *The factoring time doesn't vary directly with the length of the number
> to be factored, either. If it did, RSA would have been dead and
> buried long ago, since factoring 4096-bit numbers would require only
> eight times as much time as factoring 512-bit numbers.*

Was I've said is one bit means about 2 times the work, or less with a better algorithm, but still somewhat close to that.

So factoring a 4096 bit number takes $2^{(4096-512)}$ times [the time to factor a 512 bit number].

The point of my original post was we're faster than this, but certainly not so much.

Milan