

## Re: Surrogate factoring explained

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/4623.html>

---

**From:** JT ([jt64\\_at\\_bredband.net](mailto:jt64_at_bredband.net))

**Date:** 02/26/05

Date: 25 Feb 2005 16:16:39 -0800

"oðin" <[oðin@ragnarok.com](mailto:oðin@ragnarok.com)> wrote in message news:<[HrOdnbj\\_38Im3YLfRVn-hA@whidbeytel.com](mailto:HrOdnbj_38Im3YLfRVn-hA@whidbeytel.com)>...  
> > > *So basically I believe that RSA numbers are 'special'.*  
> >  
> > *When people say "special" they usually mean things like strong primes*  
> > *or such...*  
>  
>  
> *There is doubt by many that even an effort to use so called strong primes is*  
> *of any use. Strong is a term that is relative to known factoring methods,*  
> *which are still not good enough to cause worry with sufficient bit size and*  
> *are not understood well enough to know exactly what makes them strong.*  
> *Besides, even so called strong primes are not that special. Using A PRNG*  
> *seems to be good enough.*

This question may seem strange, how many bits is the biggest consequent prime ever found, bigger or less then the RSA challenge.

If not is there a proof that the RSA challenge actually isn't a prime itself?

Because if it is we will have a waist of time tryin to factor it ;)

JT