

Re: Special factorization method sought

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-07/0017.html>

From: Robert Maas, see <http://tinyurl.com/uh3t> (*rem642b_at_Yahoo.Com*)

Date: 07/01/05

Date: Thu, 30 Jun 2005 23:04:55 -0700

> *From: "Pubkeybreaker" <Robert_silverman@raytheon.com>*
> *Unless of course, the numbers are *so* extremely close that*
> *difference of squares can be used. However, for even moderately*
> *large N, if $N = A*B$ and the size of A and B differs by only 1 bit,*
> *then this method is useless.*

Ah, that's good (for me) to know. So the algorithm I developed in late 1977 (after reading Martin Gardner's info about the RSA code) is quite sufficient. The user specifies the number of decimal digits desired, and a string which is the high-order decimal digits, such as the user's telephone number or social security number etc. that will be easy to remember. This template will be used as a restriction on $p*q$ so that when it's published it'll be obvious whose code is being published, and so two different users would ever come up the same exact product by accident. After that number-of-digits and high-order prefix is specified, the program synthesizes a random prime that has about half the number of digits. Then it performs interval-arithmetic division, in contracting mode instead of the usual expanding mode, to find what range the other prime number must be such that the product is guaranteed to have the correct number of digits and correct high-order prefix. Then it synthesizes that second prime in that range. The range is so wide that it's extremely unlikely that the two primes would be so close as to make factorization by square root method practical.

And if you are really worried about the two primes accidentally being too close, for the range of the first prime, instead of taking the full range near the square root of the desired product, you can take only the lower half of it, minus the part that is too near the square root. The other prime then will be guaranteed in the upper half also far enough from the square root. For example, if your phone number is 1-414-213-5624 (if you can't guess where I came up with that particular fake phone number, you shouldn't be reading this newsgroup), and you want a 100-digit product, then the template for the product is
14142135624xx
xx
so you want two primes, each appx. 50-digits, with the first bounded sufficiently below the square root of the lower bound of the above

