

Re: Special factorization method sought

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-06/2104.html>

From: Risto Lankinen (rlankine_at_hotmail.com)

Date: 06/29/05

Date: Wed, 29 Jun 2005 13:33:53 GMT

"Pubkeybreaker" <Robert_silverman@raytheon.com> wrote in message news:1120049302.976799.253360@o13g2000cwo.googlegroups.com...

> *It is called the General Number Field Sieve.*

>

> *This is the best that is known.*

Even for integers having "nearly equal size" factors?

Why am I asking? If you take 'n' and multiply it with a 2^b where 'b' is the highest integer for which it is true that $n/9 > 2^b$, then $n \cdot 2^b$ is guaranteed to split into two factors of "nearly equal size" iff 'n' has non-trivial factors. [And, if you multiply by highest 'b' for which $n > 2^b$ you will include the trivial factoring $n \cdot 1$ into the result set, allowing 'n' even to be a prime, but that is counterproductive when the aim is to factor 'n'].

Example: To factor $7 \cdot 1009 = 7063$, find "nearly equal size" factors of $512 \cdot 7063$, which are 1792 and 2018 . After the trivial removal of 2's you're done.

It's granted, that the magnitude of the number-to-factor becomes much larger, but it also becomes "structured". One obvious exploitation of the structuredness is to use some modified square root algorithm, but I wonder if there's a way to do much better...

I posted an algorithm implementing this in a rudimentary manner a few days ago, but it didn't raise much interest. Here's the link, anyway:

http://groups.google.fi/groups?selm=%254cue.2751%24_k2.49910%40news2.nokia.com

– Risto –