

## Re: Special factorization method sought

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-06/2106.html>

---

**From:** Pubkeybreaker (*Robert\_silverman\_at\_raytheon.com*)

**Date:** 06/29/05

Date: 29 Jun 2005 07:23:29 -0700

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

> *This is the best that is known.*

Even for integers having "nearly equal size" factors?

\*Especially\* for numbers having nearly equal size factors.

For other numbers, ECM is available.

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.

Its run time will be  $O((A+B)/2 - \text{SQRT}(N))$ . But you specified  $x > y > x/2$

and this is not close enough in general.

For example. Suppose  $N$  is only 100 digits.  $A$  and  $B$  are both 50 digits.

$A$  and  $B$  match to their first 5 significant digits. Say  $A \sim 5.43217 \times 10^{45}$  and

$B \sim 5.43211 \times 10^{45}$ . Then the work to split them by difference of squares

is about  $10^{39}$ . i.e. hopeless. And these are very close together.

Even if

$A$  and  $B$  match to (say) the first 9 or 10 digits, the work will be prohibitive.