

Christof Paar, Assistant Professor
Cryptography and Information Security (CRIS) Group
ECE Dept., WPI, 100 Institute Rd., Worcester, MA 01609, USA fon:
(508) 831 5061 email: christof@ece.wpi.edu fax: (508) 831 5491
www: <http://ee.wpi.edu/People/faculty/cxp.html>

Subject: Factorization of RSA-140 with the Number Field Sieve From:
herman@cwil.nl (Herman J.J. te Riele) Date: 02/04/1999 04:52 AM Eastern
Standard Time Message-id:

On February 2, 1999, we found that

RSA-140 =
21290246318258757547497882016271517497806703963277216278233383215381949984056495
911366573853021918316783107387995317230889569230873441936471

can be written as the product of two 70-digit primes:

3398717423028438554530123627613875835633986495969597423490929302771479
*
6264200187401285096151654948264442219302037178623509019111660653946049

Primality of the factors was proved with the help of two different
primality proving codes. An Appendix gives the prime decompositions of
 $p \pm 1$. The number RSA-140 is taken from the RSA Challenge list
(<http://www.rsa.com/rsalabs/html/factoring.html>).

This factorization was found using the Number Field Sieve (NFS)
factoring algorithm, and beats the 130-digit record that was set on
April 10, 1996, also with the help of NFS [Cetal].

The amount of computer time spent on this new 140-digit NFS-record is
prudently estimated to be equivalent to 2000 mips years. For the old
130-digit NFS-record, this effort is estimated to be 1000 mips years.

For both numbers, lower "could-have-done-it-in" estimates,
based on a better use of the lattice siever, are:

500 mips years for RSA-130 and 1500 mips years for RSA-140.

For information about NFS, see [LL]. For additional information,
implementations and previous large NFS factorizations, see [DL, E1,
E2, GLM].