New record in the area of prime number decomposition of cryptographically important numbers

8 January 2010, by Florence Luy

An international team of scientists from EPFL (Switzerland), INRIA (France), NTT (Japan), CWI (The Netherlands) and Bonn University (Germany), has obtained the prime factors of the RSA challenge number RSA-768, using the Number Field Sieve.

The calculation took less than 2000 core years on modern CPUs.

Extrapolating the trend from previous records in this area (512-bit in 1999, 663-bit in 2005, and the current 768-bit in 2009), it is reasonable to expect that 1024-bit keys will exhibit a similar degree of vulnerability within the next decade.

The result thus underlines the importance to adopt the new cryptographic key size standards that recommend phasing out usage of currently popular 1024-bit RSA keys. However, it also indicates that, assuming similar resources, users do not incur undue risks by continued usage of 1024-bit RSA keys during the next few years of transition to higher security levels.

The software used was to a considerable extent based on a package developed in the early 2000s at the Mathematics Institute at Bonn University, and further developed by the present collaborators. EPFL's Laboratory for Cryptologic Algorithms acted as main organizer, central data collection point, and contributed approximately a third to the overall computational effort.

More information:
-- Paper: documents.epfl.ch/users/l/le/l … ic/papers/rsa768.txt
-- General number field sieve: en.wikipedia.org/wiki/General_number_field_sieve
-- RSA Factoring Challenge: en.wikipedia.org/wiki/RSA_Challenge

Provided by Ecole Polytechnique Fédérale de Lausanne