I wrote this library when I finally managed to understand the ins and outs of factoring large integers using advanced sieving methods (it took years).

Current versions use just about every modern factorization algorithm available. These include GMP-ECM , a very fast implementation of the self-initializing quadratic sieve with one or two large primes, and a complete implementation of the number field sieve . The core code is organized as a library with a lightweight API that allows easy integration with other applications.

Most current development focuses on the number field sieve. This is divided into three stages; the first two stages are fairly mediocre right now compared to the state of the art embodied in GGNFS , but the final stage is the fastest and most robust code of its kind that's publicly available. It has helped complete all of the most recent factorizations undertaken by NFSNET , and has also helped factor a 180-digit general number and a 273-digit special number (2^908+1). If you need to factor really big numbers, you should use both GGNFS and Msieve. Ask me or the GGNFS user group if you need help.

Msieve is under active development, thanks to generous support and testing from lots of people, many of whom can be reached at Mersenn

eforum .
Source code and Windows binaries are now hosted on
the Msieve SourceForge Page