Summer School - Number Theory for Cryptography

F. Morain

Tutorial, 2013/06/27

Powerful factorization has to be tried. The work can be distributed and linear algebra easily done with SAGE.

1. Implement CFRAC.

2. Implement QS.

3. Implement MPQS.