

In this work we study the number field sieve algorithm. Our main focus is on its theoretical background. We present all important theorems which are needed for a full understanding of the algorithm. We also describe the most widely used implementation of the parts of the algorithm and we discuss in which situation they should be used. At the end we show results from measurements of sieving phase on the implementation which was written for our Department of Algebra.