Many of today’s cryptographic systems are based on the discrete logarithm problem, e.g. the Diffie-Hellman protocol. The number field sieve algorithm (NFS) is the algorithm solving the problem of factorization of integers, but latest works show, it can be also applied to the discrete logarithm problem.

In this work, we study the number field sieve algorithm for discrete logarithm and we also compare the NFS for discrete logarithm with the NFS for factorization. Even though these NFS algorithms are based on the same principle, many differences are found.