1.	Record Nr.	UNISA996466661203316
	Titolo	The development of the number field sieve / / A. K. Lenstra, H. W. Lenstra, Jr., editors
	Pubbl/distr/stampa	Berlin ; ; Heidelberg : , : Springer-Verlag, , [1993] ©1993
	ISBN	3-540-47892-2
	Edizione	[1st ed. 1993.]
	Descrizione fisica	1 online resource (VIII, 140 p.)
	Collana	Lecture Notes in Mathematics ; ; Volume 1554
	Disciplina	512.73
	Soggetti	Sieves (Mathematics)
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di contenuto	The number field sieve: An annotated bibliography -- Factoring with cubic integers -- The number field sieve -- The lattice sieve -- Factoring integers with the number field sieve -- Computing a square root for the number field sieve -- A general number field sieve implementation.
	Sommario/riassunto	The number field sieve is an algorithm for finding the prime factors of large integers. It depends on algebraic number theory. Proposed by John Pollard in 1988, the method was used in 1990 to factor the ninth Fermat number, a 155-digit integer. The algorithm is most suited to numbers of a special form, but there is a promising variant that applies in general. This volume contains six research papers that describe the operation of the number field sieve, from both theoretical and practical perspectives. Pollard's original manuscript is included. In addition, there is an annotated bibliography of directly related literature.