1.	Record Nr.	UNINA9910479867703321
	Autore	Koblitz Neal
	Titolo	A Course in Number Theory and Cryptography [[electronic resource] /] / by Neal Koblitz
	Pubbl/distr/stampa	New York, NY : , : Springer New York : , : Imprint : Springer, , 1994
	ISBN	1-4419-8592-1
	Edizione	[Second Edition.]
	Descrizione fisica	1 online resource (X, 235 p.)
	Collana	Graduate Texts in Mathematics, , 0072-5285 ; ; 114
	Classificazione	10-01 94A05 10H99 11-01
	Disciplina	512.7
	Soggetti	Number theory Number Theory
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
	Nota di contenuto	I. Some Topics in Elementary Number Theory -- 1. Time estimates for doing arithmetic -- 2. Divisibility and the Euclidean algorithm -- 3. Congruences -- 4. Some applications to factoring -- II. Finite Fields and Quadratic Residues -- 1. Finite fields -- 2. Quadratic residues and reciprocity -- III. Cryptography -- 1. Some simple cryptosystems -- 2. Enciphering matrices -- IV. Public Key -- 1. The idea of public key cryptography -- 2. RSA -- 3. Discrete log -- 4. Knapsack -- 5 Zero-knowledge protocols and oblivious transfer -- V. Primality and Factoring -- 1. Pseudoprimes -- 2. The rho method -- 3. Fermat factorization and factor bases -- 4. The continued fraction method -- 5. The quadratic sieve method -- VI. Elliptic Curves -- 1. Basic facts -- 2. Elliptic curve cryptosystems -- 3. Elliptic curve primality test -- 4. Elliptic curve factorization -- Answers to Exercises. .
	Sommario/riassunto	. . . both Gauss and lesser mathematicians may be justified in rejoicing that there is one science [number theory] at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean. - G. H. Hardy, A Mathematician's Apology, 1940 G. H. Hardy would have been surprised and probably displeased

with the increasing interest in number theory for application to "ordinary human activities" such as information transmission (error-correcting codes) and cryptography (secret codes). Less than a half-century after Hardy wrote the words quoted above, it is no longer inconceivable (though it hasn't happened yet) that the N. S. A. (the agency for U. S. government work on cryptography) will demand prior review and clearance before publication of theoretical research papers on certain types of number theory. In part it is the dramatic increase in computer power and sophistica- tion that has influenced some of the questions being studied by number theorists, giving rise to a new branch of the subject, called "computational number theory. " This book presumes almost no background in algebra or number the- ory. Its purpose is to introduce the reader to arithmetic topics, both ancient and very modern, which have been at the center of interest in applications, especially in cryptography. For this reason we take an algorithmic approach, emphasizing estimates of the efficiency of the techniques that arise from the theory.

2.	Record Nr.	UNINA9910779503303321
	Autore	Storozhuk A. IU (Anna IUrevna)
	Titolo	Color [[electronic resource]] : ontological status and epistemic role / / Anna Storozhuk
	Pubbl/distr/stampa	New York., : Nova Science Publishers, 2010
	ISBN	1-61668-608-1
	Descrizione fisica	1 online resource (78 p.)
	Collana	Chaos and complexity research compendium ; ; v. 1 Eye and vision research developments
	Disciplina	111/.1
	Soggetti	Color (Philosophy) Color vision
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	The physical properties of color and its influence on the organism -- The source of the myths about experience : the principle of the being and thinking identity.