

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Record Nr.           | UNINA9910479867703321                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Autore                  | Koblitz Neal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Titolo                  | A Course in Number Theory and Cryptography [[electronic resource] ] /<br>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<br>94A05<br>10H99<br>11-01                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Disciplina              | 512.7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Soggetti                | Number theory<br>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<br>index.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Nota di contenuto       | I. Some Topics in Elementary Number Theory -- 1. Time estimates for<br>doing arithmetic -- 2. Divisibility and the Euclidean algorithm -- 3.<br>Congruences -- 4. Some applications to factoring -- II. Finite Fields<br>and Quadratic Residues -- 1. Finite fields -- 2. Quadratic residues and<br>reciprocity -- III. Cryptography -- 1. Some simple cryptosystems -- 2.<br>Enciphering matrices -- IV. Public Key -- 1. The idea of public key<br>cryptography -- 2. RSA -- 3. Discrete log -- 4. Knapsack -- 5 Zero-<br>knowledge protocols and oblivious transfer -- V. Primality and<br>Factoring -- 1. Pseudoprimes -- 2. The rho method -- 3. Fermat<br>factorization and factor bases -- 4. The continued fraction method --<br>5. The quadratic sieve method -- VI. Elliptic Curves -- 1. Basic facts --<br>2. Elliptic curve cryptosystems -- 3. Elliptic curve primality test -- 4.<br>Elliptic curve factorization -- Answers to Exercises. . |
| Sommario/riassunto      | . . . both Gauss and lesser mathematicians may be justified in rejoic-<br>ing that there is one science [number theory] at any rate, and that their<br>own, whose very remoteness from ordinary human activities should<br>keep it gentle and clean. - G. H. Hardy, A Mathematician's Apology,<br>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 sophistication 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 theory. 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.           | UNINA9910715309903321                                                                                            |
| Titolo                  | Failure of remote shutdown system instrumentation because of incorrectly installed components                    |
| Pubbl/distr/stampa      | Washington, D.C. : , : United States Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, , 1991 |
| Descrizione fisica      | 1 online resource                                                                                                |
| Collana                 | Information notice ; ; 91-53                                                                                     |
| Soggetti                | Nuclear reactors - Shutdown<br>Nuclear power plants - Instruments                                                |
| Lingua di pubblicazione | Inglese                                                                                                          |
| Formato                 | Materiale a stampa                                                                                               |
| Livello bibliografico   | Monografia                                                                                                       |
| Note generali           | "September 4, 1991."                                                                                             |

