1. Record Nr. UNINA9910798486803321

| Autore | Diekert Volker < <br> Titolo |
| :--- | :--- |
| Discrete algebraic <br> groups / / Volker |  |
| Pubbl/distr/stampa | Berlin, Germany |
|  | ©2016 |
| ISBN | $3-11-041333-7$ |
|  | $3-11-041632-8$ |


| Descrizione fisica | online resource (354 pages) : illustrations |
| :--- | :--- |
| Collana | De Gruyter Textbook |
| Disciplina | $511.3 / 3$ |
| Soggetti | Ordered algebraic structures |
|  | Algorithms |
|  | Computer science - Mathematics |
|  | Cryptography |


| 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 and index. |
| Nota di contenuto | Frontmatter -- Preface -- Contents -- 1. Algebraic structures -- 2. Cryptography -- 3. Number theoretic algorithms -- 4. Polynomial time primality test --5. Elliptic curves -- 6. Combinatorics on words -- 7. Automata -- 8. Discrete infinite groups -- Solutions to exercises -Bibliography -- Index |

Sommario/riassunto

The idea behind this book is to provide the mathematical foundations for assessing modern developments in the Information Age. It deepens and complements the basic concepts, but it also considers instructive and more advanced topics. The treatise starts with a general chapter on algebraic structures; this part provides all the necessary knowledge for the rest of the book. The next chapter gives a concise overview of cryptography. Chapter 3 on number theoretic algorithms is important for developing cryptosystems, Chapter 4 presents the deterministic primality test of Agrawal, Kayal, and Saxena. The account to elliptic curves again focuses on cryptographic applications and algorithms. With combinatorics on words and automata theory, the reader is introduced to two areas of theoretical computer science where
semigroups play a fundamental role. The last chapter is devoted to combinatorial group theory and its connections to automata.

