Techniques of Algebraic Geometry play an increasing role in the theory of Error Correcting Codes as well as in Cryptography, and many recent books study these relationships. For example the book of H. Stichtenoth, second edition [Graduate Texts in Mathematics 254. Berlin: Springer. (2009; Zbl 1155.14022)] examines the interplay between algebraic curves (or function fields of one variable) and algebraic-geometry codes, while the book of H. Cohen et al. [Handbook of elliptic and hyperelliptic curve cryptography. Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC. (2006; Zbl 1082.94001)] is devoted to Cryptography with elliptic and hyperelliptic curves. The present book also shows these classical applications and others due to the authors, both well known researchers in the areas of Finite Fields, Cryptography and Error Correcting Codes.

The first four chapters can be viewed as a course on algebraic curves and their function fields with particular emphasis on the case of a finite ground field (another recent reference on algebraic curves over finite fields is the book, with that title, of J. W. P. Hirschfeld, G. Korchmáros and F. Torres [Princeton Series in Applied Mathematics. Princeton, NJ: Princeton University Press. (2008; Zbl 1200.11042)]. The authors argue that detailed proofs of the correspondence between nonsingular projective curves over finite fields and global function fields are difficult to find and, in their words, “one contribution of our book is to fill this gap by giving complete proofs of these results”.

Chapter 5 studies the interplay between algebraic curves and coding theory. Besides the study of Goppa’s algebraic-geometry codes the chapter details some generalizations of them, as the NXL (Niederreiter, Xing and Lam) codes, the XNL (Xing, Niederreiter and Lam) codes and the functional codes and finally shows applications of global function fields to digital nets.

The last Chapter 6 is concerned with cryptographic constructions related to algebraic curves (mainly elliptic and hyperelliptic curves) defined over a finite field as well as some connections between Coding Theory and Cryptography as the McEliece and Niederreiter public key cryptosystems and some applications of global functions fields to the construction of fingerprints schemes for the protection of the intellectual property.

Reviewer: Juan Tena Ayuso (Valladolid)

MSC:
14–02 Research exposition (monographs, survey articles) pertaining to algebraic geometry
14G15 Finite ground fields in algebraic geometry
14G50 Applications to coding theory and cryptography of arithmetic geometry
14H05 Algebraic functions and function fields in algebraic geometry
94A60 Cryptography
94B27 Geometric methods (including applications of algebraic geometry) applied to coding theory

Keywords:
finite fields; algebraic function fields; algebraic curves; Riemann-Roch theorem; rational places; coding theory; algebraic-geometry codes; function-field codes; elliptic and hyperelliptic curve cryptography; McEliece and Niederreiter cryptosystems; frameproof codes