Πεπερασμένα Σώματα & Κρυπτογραφία

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}$$

$\mathbb{F}_{p^d}$
|
$\mathbb{F}_p$

$y^2 = x^3 + ax + b$

Γιάννης Αντωνιάδης
Αριστείδης Κοντογεώργης

METADATA

Title: Finite Fields and Cryptography

Other Titles: -

Language: Greek

ISBN: 978-618-82124-6-6

Subject: MATHEMATICS AND COMPUTER SCIENCE

Keywords: Finite Fields / Cryptography / Elliptic Curves / Computational Number Theory

• • •

Abstract

The proposed book refers to the applications of Number Theory in cryptography. Beyond the elementary constructions available in the literature, it will provide an introduction to the new field of elliptic curve cryptography, for which there is not yet an accessible introduction in the Greek literature. The book corresponds to the content of the course "Finite Fields and Cryptography," as it is taught to the students of the Mathematics Department at the University of Athens (UOA). However, we believe it will also be useful in the teaching of other cryptography courses in Mathematics, Computer Science, and Engineering departments.