Download Algebraic Curves And Cryptography

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.Like its bestselling predecessor, Elliptic Curves: Number Theory and Cryptography, Second Edition develops the theory of elliptic curves to provide a basis for both number theoretic and cryptographic applications.Overview. Welcome to the Centre for Applied Cryptographic Research (CACR) at the University of Waterloo, a joint project between the University, the Federal Government of Canada, and the following corporations:Although the formal definition of an elliptic curve is fairly technical and requires some background in algebraic geometry, it is possible to describe some features of elliptic curves over the real numbers using only introductory algebra and geometry.