Elliptic Curves and Their Applications to Cryptography

By Enge, Andreas

Book Condition: New. Publisher/Verlag: Springer, Berlin | An Introduction | Since their invention in the late seventies, public key cryptosystems have become an indispensable asset in establishing private and secure electronic communication, and this need, given the tremendous growth of the Internet, is likely to continue growing. Elliptic curve cryptosystems represent the state of the art for such systems. Elliptic Curves and Their Applications to Cryptography: An Introduction provides a comprehensive and self-contained introduction to elliptic curves and how they are employed to secure public key cryptosystems. Even though the elegant mathematical theory underlying cryptosystems is considerably more involved than for other systems, this text requires the reader to have only an elementary knowledge of basic algebra. The text nevertheless leads to problems at the forefront of current research, featuring chapters on point counting algorithms and security issues. The Adopted unifying approach treats with equal care elliptic curves over fields of even characteristic, which are especially suited for hardware implementations, and curves over fields of odd characteristic, which have traditionally received more attention. Elliptic Curves and Their Applications: An Introduction has been used successfully for teaching advanced undergraduate courses. It will be of greatest interest to mathematicians, computer scientists, and...

READ ONLINE
[5.72 MB]

Reviews

Very beneficial to all category of folks. We have study and that i am sure that i will planning to go through yet again again in the future. Its been printed in an extremely straightforward way in fact it is just soon after i finished reading this pdf where actually changed me, alter the way i really believe.
-- Emmett Mann

Comprehensive information! Its this sort of great go through. It really is rally interesting throgh studying time. I am just quickly can get a satisfaction of looking at a created pdf.
-- Alexandra Weissnat