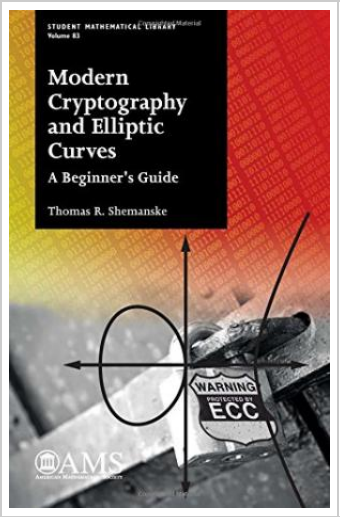




# Modern Cryptography and Elliptic Curves: A Beginner s Guide (Paperback)

By Thomas R. Shemanske

American Mathematical Society, United States, 2017. Paperback. Condition: New. Language: English . Brand New Book. This book offers the beginning undergraduate student some of the vista of modern mathematics by developing and presenting the tools needed to gain an understanding of the arithmetic of elliptic curves over finite fields and their applications to modern cryptography. This gradual introduction also makes a significant effort to teach students how to produce or discover a proof by presenting mathematics as an exploration, and at the same time, it provides the necessary mathematical underpinnings to investigate the practical and implementation side of elliptic curve cryptography (ECC).Elements of abstract algebra, number theory, and affine and projective geometry are introduced and developed, and their interplay is exploited. Algebra and geometry combine to characterize congruent numbers via rational points on the unit circle, and group law for the set of points on an elliptic curve arises from geometric intuition provided by Bezout s theorem as well as the construction of projective space. The structure of the unit group of the integers modulo a prime explains RSA encryption, Pollard s method of factorization, Diffie-Hellman key exchange, and ElGamal encryption, while the group of points of an elliptic curve...



### Reviews

*This created ebook is wonderful. I could possibly comprehended everything out of this created e ebook. Its been designed in an remarkably easy way and is particularly just after i finished reading through this ebook by which basically modified me, affect the way i believe.*

-- ***Verner Langworth III***

*Very good electronic book and valuable one. It is actually writter in basic words instead of difficult to understand. I discovered this ebook from my i and dad encouraged this publication to discover.*

-- ***Prof. Jevon Frami***